ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

D1.1

Holistic Security Context Analysis

This deliverable presents the results of ANASTACIA Task 1.1. The aim of the task is to perform a holistic analysis of ANASTACIA cybersecurity approach, by analysing the various risks from a life cycle perspective, across the whole deployment from the edge to the core, combining various expertise and stakeholder perspectives.

Distribution level	[PU]
Contractual date	<30.06.2017> [M06]
Delivery date	<30.06.2017> [M06]
WP / Task	WP1 / T1.1
WP Leader	CNR
Authors	E. Cambiaso (CNR), M. Mongelli (CNR), I. Vaccari (CNR), R. Trapero Burgos (ATOS), M. Alie El-din (UTRC), D. Belabed (THALES), T. Taleb (AALTO), I. Farris (AALTO), M. A. Bou Hanana (AALTO), A. Molina Zarca (UMU), D. Rivera (MONT), K. Eunah (DG), L. Scudiero (AS).
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat SpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.anastacia-h2020.eu

ANASTACIA has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

This document only reflects the ANASTACIA Consortium's view.
The European Commission is not responsible for any use that may be made of the information it contains.

Table of contents

PUBLIC SUMMARY

ANASTACIA is a framework for the management of complex networks and systems. Following technologies and scenarios are in particular addressed: Internet of Things (IoT), Software Defined Networks (SDN), Building Energy Management System (BEMS), Multi-access Edge Computing (MEC), also considering Network Function Virtualization (NFV) and Policy Based Management aspects.

The main aims of the ANASTACIA platform are to guarantee secure data transmissions, considering that information shared on the network are sensitive by nature. Such goal requires the design, implementation and deploy of innovative and efficient protection systems, technologies and algorithms.

This deliverable provides an analysis of the technical approaches adopted to implement the framework, the innovative holistic security model, also focusing on threats and relative detection and mitigation activities and methodologies. Moreover, security policies definition approaches will be discussed, analysing the structural and decisive aspects, by making a deep study on ANASTACIA users and their activities and behaviour.

These concepts are the kernel of the holistic security approach, an innovative implementation of security systems that in the last years become extremely popular due to the detection of novel threats inside of computer networks through, e.g., behavioural user analysis, able to provide information about the source of network attacks. In this context, behavioural user analysis brings to innovative protection systems including novel and unexpected categories of attacks.

1 INTRODUCTION

In this initial chapter we will introduce the main functionalities and characteristics of the ANASTACIA project, mainly focusing on the approach adopted to implement the system/framework, on the technical aspects and on security aspects to be considered during the development of the platform.

1.1 TECHNICAL ASPECTS OF ANASTACIA

The ANASTACIA project analyses different technological aspects considered particularly important in the cyber-security field. In this initial section we will briefly introduce the technologies and notions used in ANASTACIA:

- **Cybersecurity**: field of the computer science working on threat analysis, vulnerabilities identification and management and to the risk associated to ICT assets, with the aim of protect such systems from (internal or external) cyber-attacks potentially able to create (direct or indirect) damages with impact higher than a pre-defined threshold (e.g. economic, reputation, socio-politics damages, etc.).
- **Cyber-physical systems**: ICT system able to interact in continuous way with the physical system it operates in. The system is composed of physical elements equipped with computational capabilities and it presents three characteristics ("the three C"): computational capabilities, communication and control capabilities.
- **Internet of Things (IoT)**: common life objects (e.g. fridge, TV, door sensor, video-cameras, light bulbs, weather stations, etc.) are able to communicate among themselves and with the environment by exploiting an Internet connection to exchange data in real time, without requiring external devices demanded to manage the communication.
- **Software-defined networking (SDN)**: approach used in the computer network fields to provide network administrators the ability to initialize, control, update and manage in a dynamic way the network configuration through apposite interfaces and protocols and by abstracting low level functionalities of the network nodes.
- **Network function virtualization (NFV)**: network architecture concept using IT virtualization technologies to virtualize entire classes of functions in order to design, deploy and manage networking services.

1.2 REASONS AND AIMS OF THE PROJECT

The main ANASTACIA objective is to provide security and trust on ICT systems by properly managing the constant and continuous discovery of vulnerabilities. ANASTACIA will adopt a holistic security framework addressing all the stages of the ICT systems development lifecycle. The ANASTACIA platform considers the evolution of ICT aspects such as information security, technologies and discovery of novel evolving cyber-attacks. These concepts are extremely important in the cyber-security field. In particular, considering novel threats, in case an ICT system is targeted by a 0-day attack and it is not possible to properly counter and mitigate the threat, the effects of the attack may be catastrophic. Because of this, the ANASTACIA project aims to create an elastic and dynamic protection system based on an innovative approach implementing, deploying, and providing security on data transmission and connected devices.

1.3 INTRODUCTION TO HOLISTIC SECURITY APPROACH

In the last years, holistic approaches have been widely included in the system/platform development life-cycle. Such approach focuses on analysing the entire network infrastructure, without excluding any

variable. In this document, we better describe how a holistic approach “works” and we report the main characteristics of it.

Cyber-security can be seen as a purely ICT related issue or as a legislative and regulation compliance problem. Nevertheless, it needs a new approach able to consider all the components of the system, in order to define a security plan able to effectively protect the commercial interests, the immaterial assets and the infrastructure of the organization, by protecting them from risks and threats that may potentially target the system.

1.4 REVISION HISTORY

Version	Date	Author	Description
0.1	April 19th, 2017	E. Cambiaso	First version of the document
0.2	May 23th, 2017	E. Cambiaso	Integrated contributions from other partners
0.3	May 26th, 2017	M. Mongelli	Internal review of the document
0.4	June 7 th, 2017	I. Vaccari	RC1 production
0.5	June 28th, 2017	I. Vaccari	RC2 production
0.6	June 29th, 2017	I. Vaccari E. Cambiaso	Final version production

2 HOLISTIC CYBERSECURITY APPROACH

Technology is always under development and innovation, every day new devices and novel technologies are introduced into the market and proposed to the world. The main aim of technological development is to optimize the daily lives of people, e.g. monitoring their home using a mobile device or to access into their bank account using a smartphone.

Technology has also attracted malicious users who exploit this development to gain fame or to recover important information that can subsequently sell. Cyber security is an essential element of technology since is necessary to protect devices from possible attacks by hackers. Organizations are the primary target of hackers since most of them use and exchange sensitive data every day. This realization is driven by different factors: the wide range of cyber-attacks available, the potential victims, the use of social engineering, and the role of the insider, becoming more and more important every day.

An organization can implement its defence system using different approaches, such as deciding to defend itself from a particular suite of attacks or limited access to sensitive data, but in recent studies, it has been verified that the systems are vulnerable. A very used approach with great results to prevent and manage cyber-attacks is the holistic approach. A holistic approach incorporates technical, human and physical factors relevant to detection, prevention, and correction of cyber-security vulnerabilities[1]. The main feature of this approach is to expand defence over technology mainly for two reasons: who runs the attack is a person and the attacker's goal is very often attacking a person to access the network. This approach seeks to achieve a balance between efficiency and security. A growing set of case studies are demonstrating that even the best technological solutions can be rendered ineffective by improper human action. Nevertheless, proper human behaviour enhances the capability of these same technological defences.

A holistic system uses collaboration between people, technology and physical defences to make a secure system and protect from cyber-attacks. Initially, an organization's security study is conducted, the main aim is finding vulnerabilities to define a general defence structure.

Most evaluations focus mainly on the technical aspects, performing penetration testing to ensure network security for the organization, the human and physical factors are arguably just as important. Organization must be considerate such as an association of people and processes into a physical domain rather than just a series of devices on a network, in this way is possible to gain an accurate perspective of an organization's systems and the collaboration between the entities in order to understand functionality of the organization. To do this, it must be performed a study of strengths and weaknesses of all aspects present in an organization's security by analyzing internal staff, physical defences and the cyber security awareness and accountability of the staff. The initial step of this procedure is to identify critical information, that is, information that if stolen, modified, or inaccessible, can lead to serious losses to the organization. The data used within an organization contains very delicate information about activities carried out, personal data of employees or transactions carried out with external identities as customers or suppliers. The decision to protect data is crucial as defending all types of data is very complex and even if there is a system capable of protecting all data, it would be a unsafe system. The decision-making phase of which types of data to protect is very delicate and needs to be carried out accurately. Once the definition of the data to be protected has been completed, the next step involves deciding who can physically access the areas where data or network devices are contained. If everyone had access to these devices, a malicious user could damage access to data by physically attacking the server or network infrastructure.

A very important step to creating a solid and compact defence system is to spread rules and roles to employees. Organizational employees need to know what they can and what they cannot do, and what are the consequences for incorrect or unacceptable behaviours. Cyber security governance represents the best

[1] http://www.securitymagazine.com/blogs/14-security-blog/post/87239-the-argument-for-holistic-cybersecurity

approach to do this, since governance is a critical element of cyber security awareness. A particular situation may arise when a user inflicts a cyber breach through involuntary action. Since most of the damage is caused by these situations, organizations need to inform employees in detail about the actions to be taken, as involuntary damage can lead to serious losses.

In recent years, it has been noted that most of cyber security problems detected on computer systems have been initiated by human activities. A solution to this problem was sought, the best way to mitigate this risk is through cyber security training that creates awareness and hardens personnel to attack. Without informing users of malicious actions that attackers can make to access the network, employees are at risk of manipulation and exploitation through spear-phishing or social engineering efforts aimed at stealing network credentials. One of the first things to understand about the insider threat is that it can be someone acting intentionally or unintentionally. Often, an insider is seen as an external user who wants to severely damage the organization's IT system, but most of the time users are providing involuntary access to malicious users. That is to say, the insiders cause the most of the damages by accessing sensitive data creating serious damage to the system. Extended access to data can allow insiders to create devastating damages for the system and at the same time cover up their tracks for not being discovered.

Even in these cases, the solution can instruct users not to be exploited by external users to provide network access credentials. The detection of malicious insiders can be done by analysing online activity, downloaded or transferred files, and badge records. The analysis must be made to monitor users and prevent any kind of attack from inside the system. An important consideration regarding the insider threat issue is the balance between security and employee privacy: it is generally known that there is no expectation of privacy when using an organization’s network and devices, nevertheless, employee monitoring is an area that many organizations prefer to avoid. Nowadays, any computer system is attacked by malicious users, then it is necessary to implement an attack detection system and a response plan to avoid damaging the system. The best way is to recognize the impact, own the risk, educate shareholders and partners of the risk, have a validated incident response plan, and execute that plan immediately.

The last but not the least important factor to be considered in the holistic approach is the moral aspect within the organization. If users are all with a positive mindset, loyal to their colleagues and their work, they are definitely less motivated to do damage to the business or to colleagues. Accordingly, organizational culture both creates and reinforces a security culture. The interrelationship and interdependence of organizational and security cultures, of people and devices, and devices and physical defences underlines the need for a holistic approach to cyber security.

2.1 HOLISTIC CYBERSECURITY APPROACH FORMALIZATION

In order to define the structure of the holistic approach, the first step involves the study of a possible implementation of this interesting defense system by cyberattacks. An interesting holistic framework is developed by Issa Atoum, Ahmed Otoom and Amer Abu Ali for cyber security environment. Every entity tries to protect their system defining a cyber security strategies (CSSs). These strategies are based on three main processes: formulation, strategy implementation and strategy evaluation. [Atoum, 2014] proposed a framework that implements a strategy implementation process.

The holistic approach has three main aims: first is to ensure early detection of likely threats and mitigate risks related to information systems and critical infrastructures, second is to enable decision-makers to take necessary actions once needed and the last is to be able to implement security solutions that involve vast numbers of stakeholders, including private entities, government entities and citizens.

The holistic cyber-security implementation framework (HCS-IF) aims to provide a core structure for a general approach to implement CSSs. HCS-IF is implemented by several processes sequentially executed one after the other, can be collected in five main steps (see Figure 1):

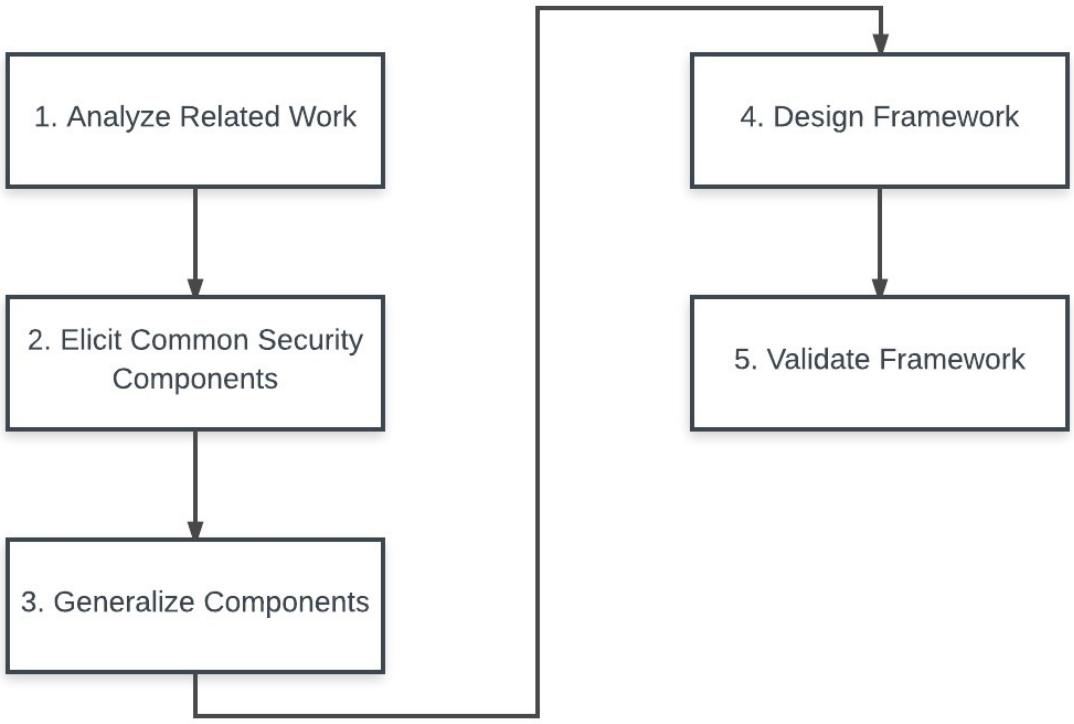

Figure 1 - A sample holistic approach for cyber-security

Accordingly to the figure, following steps are involved:

1. The initial phase conducts a study of the current state of defense systems in cyber security in national or organizational environments, focusing on guidelines and strategies used.
2. Elicit common security components: in this phase, common cyber security components are extracted. High-level security features are extracted, not analyzing the technical details of the implementation. The result of this phase is a series of features inherent in the defense from cyber-attacks that the system must have.
3. Generalize components: the data collected in the previous steps are processed by eliminating duplicates and generating common solutions to different problems.
4. At this stage, the framework is implemented using the holistic approach to achieve the aims required in the previous phases and to ensure the required security features.
5. In the last phase, the HCS-IF is compared with related frameworks.

2.2 HCS-IF

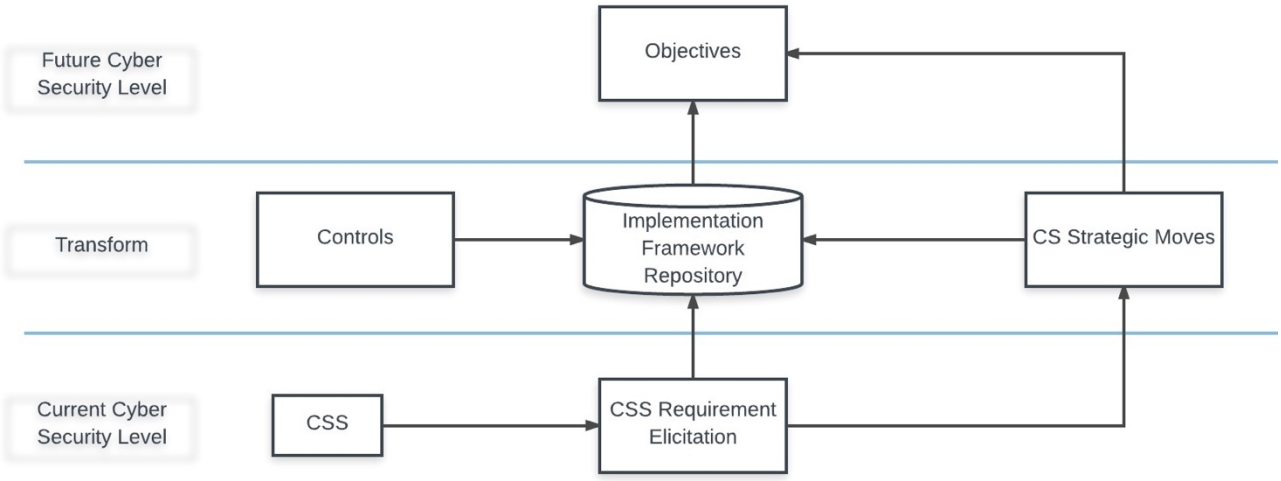

Figure 2 - HCS-IF components

The HCS-IF, shown in Figure 2, has the following major core components: CSS, requirement elicitation, strategic moves, controls, security objectives and implementation framework repository. The main goal of the HCS-IF is to analyze the CSS, extrapolate the requirements and turn them into strategic moves. These strategic moves are executed under the defined framework in order to reach the defined security objectives.

2.2.1 CSS

CSSs are based on assessments to the current information security status. These CSSs recognize the malicious threats and may include some guidelines of how to deal with cyber security threats.

2.2.2 Requirement elicitation

Requirement elicitation (RE) is a well-known sector of the software engineering field and it is used in HCS-IF to convert the CSS into a set of security requirements. The aim is to broken the CSS into manageable requirements.

2.2.3 Cyber security strategic moves

Cyber security strategic moves are actions taken to reach one or more cyber security aims. The strategic moves identify the actions to be taken to achieve a security objective of interest. This component is subdivided into different parts, as shown in Figure 3.

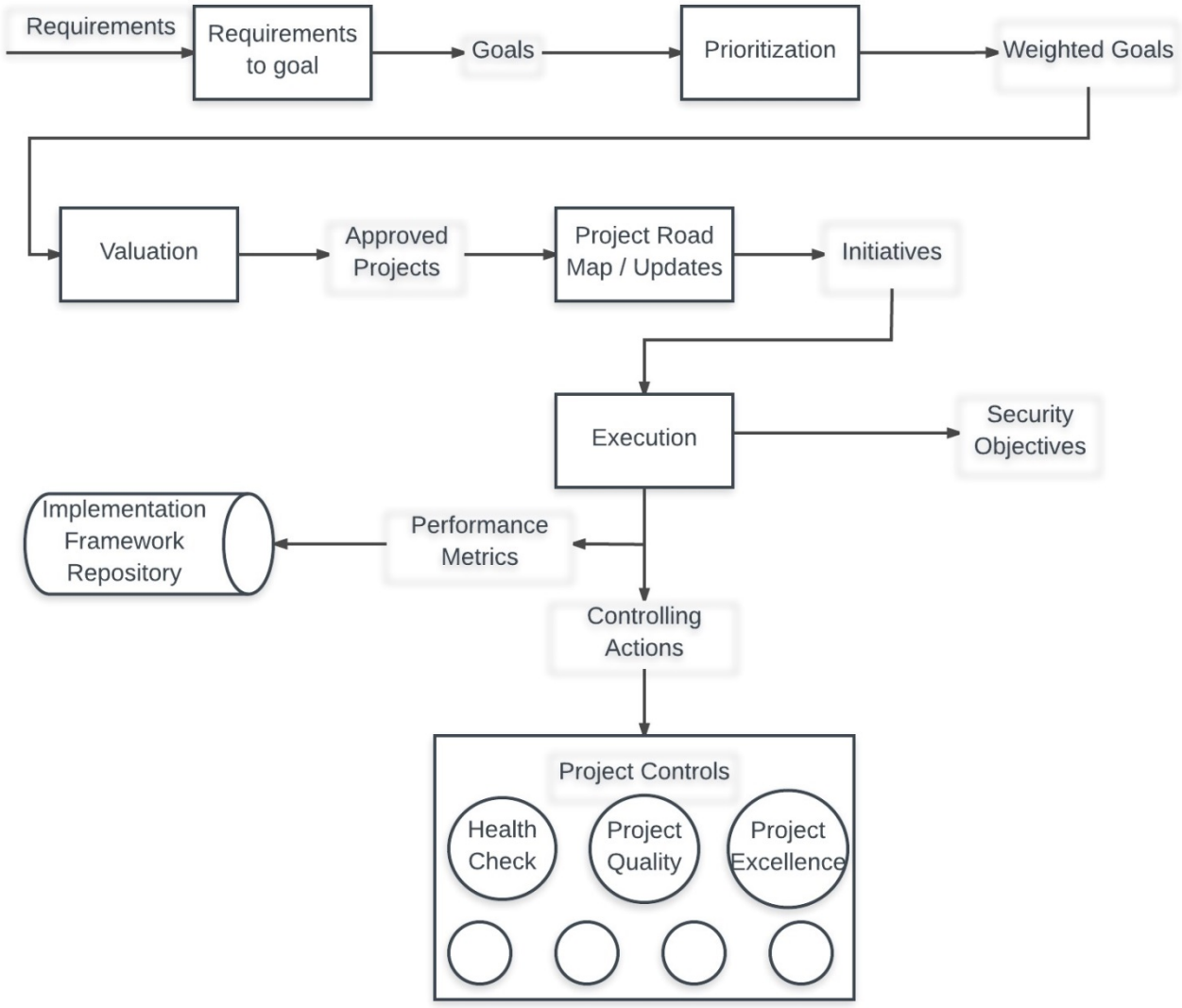

Figure 3 - Cyber-security strategic moves

Accordingly to the figure, following activities are executed:

- **Convert requirements to goals**
  Requirements are converted to SMART goals to facilitate measuring achievements, CSSs are often written in natural language because it can help to identify potential goals.
- **Prioritize goals**
  At this stage, priorities are assigned to the various goals. There are several ways to prioritize, an efficient way can be to evaluate the importance and weight of the target on the overall system.
- **Security valuation**
  The goals are often implemented by one or more projects, the purpose of this phase is to approve project initialization.

2.2.3.1 Build/update project road map

Build a road map of projects to optimize the development phase and get the best results in the shortest possible time.

2.2.4 Controls

Controls are used to manage and monitor implementation of an organization's behaviour to achieve security targets. They allow for predictive, corrective and decision-making actions. The various types of controls are reported:

- Governance: Governance controls govern the CSS implementation that required a governance entity called Cyber Security Agency (CSA). The CSA manages and monitors implementation. Governance controls are composed by:
  - CS Performance Management Control: Manages the chain of command between the entities involved.
  - Regulation Regime Control: it allows enforcing security policies and application-related legislations.
  - International Cooperation Control: Allows you to monitor different aspects of security across continents
- Strategic controls: they should allow decision-makers to determine whether the CSA is achieving objectives and enable them to make any necessary actions as early as possible during the implementation process.
- Audit controls: Are mainly used for two purposes: check the mature security level and find the difference between the original CSS and the actual implementation.
- Framework controls: the HCS-IF controls are presented to provide a means to manage the framework itself.

2.2.4.1 Business Control

This type of controls is mainly used to ensure the correct execution of operational activities by collaborating with others.

2.2.5 Validating the HCS-IF

Although several frameworks have been implemented to increase cyber security [Soomro, 2016; James, 2016], most of them focus on specific domains or entities, while HCS-IF is a type of approach that aims to increase overall cyber security.

A number of features have been defined, extracted from previous studies, with which to compare FCS-IF with previous security system deployments.

- Resilience: it represents the ability of the framework to be agile, flexible and able to deal with unpredictable changes in technology, environment, attack methods, etc.
- Measure performance: it is the ability to measure performance of security initiatives effectively at various organization levels.
- Compliance: it follows known standards or best practices and let the cyber security implementation framework manage differences between different standards.
- Measure security level: it is used to define the security level achieved at a particular time period.
- Identify gaps in CSS document: the framework should be able to detect if CSS needs further amendments in case it does not guarantee the achievement of the required security level.
- Implementation level: it shows the need of a framework that can be implemented at the national level.

2.2.6 Comparison

HCS-IF proposed provides greater security assurance as it has been implemented using a holistic approach. Accordingly to the table below, the frameworks is divided into the following categories, representing

security system implementation analysed by different sectors and differing one to the other by the exchanged data type, data to be protected or network structure:

- Management and Governance: Information security frameworks usually target the management perspective of information security.
- Guidelines: Many frameworks provide guidelines to facilitate the deployment of security systems.
- Dedicated Generic: There are several frameworks implemented for specific issues or entities.
- Generic framework: There are general framework for implementing security strategies.
- Provider specific: Some proprietary implementations have been created for security systems, most known are IBM security framework and Oracle Reference Architecture (ORA)
- Open architectures: There are various available enterprise architecture (EA) frameworks that vary in completeness, visual aspects, simplification and representation.

These categories are compared with the main features of the holistic HCS-IF approach.

Criterion/ Framework Category	Resilience	Measure performance	Compliance	Measure security level	Identify Gaps	Holistic implementation level
Management and Governance	Yes	No	No	No	No	No
Guidelines	Yes	No	No	Yes	No	Yes
Dedicated	No	No	Yes	No	No	Yes
Generic	No	Yes	No	No	No	Yes
Provider specific	Yes	Yes	Yes	Yes	No	No
Open architerctures	Yes	Yes	Yes	Yes	No	No
HCS-IF	Yes	Yes	Yes	Yes	Yes	Yes

Table 1 - Comparison between different cyber-security framework categories

3 User Perspective Analysis

In this section, we will report the user perspective analysis of the holistic cyber-security investigation accomplished. We focus on Building Energy Management Systems (BEMS), Multi-access Edge Computing (MEC), and Internet of Things (IoT) scenarios, described in the following.

3.1 Building Energy Management System (BEMS)

Automatic control of electrical components in buildings has become a necessary task for any energy management system (EMS) in order to achieve optimal performance. The aim of a modern EMS is to enhance the functionality of interactive control strategies leading towards energy efficiency and a more user friendly environment. The EMS operates several building systems, such as the supervisory control and data acquisition (SCADA), which controls the smart-grid of one or more buildings, and the building management system (BMS), which controls the building heating demand, access control, security system, fire alarm system, etc. Cyberattacks on EMS can lead to significant financial impact and safety risk. Cyberattacks on EMS can lead to significant financial impact, when EMS becomes part of the building network, where the possibility of EMS cyber-attack increases. The most common attack threats to EMS are man-in-the-middle (MiTM) and denial-of-services (DoS). Where MiTM manipulates the critical sensors and actuation values to impact the energy usage of the EMS, e.g., manipulating the building boiler set-point by a negative offset of 5 degrees can increase the building energy consumption by 8% [Paridari, 2016]. DoS can be used to shut-down the energy supply system for critical infrastructures. The main challenging for end-user in developing a security system for EMS is protecting and monitoring the massive vulnerability points introduced by connecting several heterogynous systems such as network, data-base, physical environment, etc. In addition, existing methods for EMS cyber-security are mainly based on running tests and benchmarks to evaluate the possible cyber-attacks and their impact [Gold, 2009]. These methods require expert knowledge to manually perform the tests and attack assessment. There is currently no end-to-end framework that covers the main steps in EMS cyber-security design flow. EMS is typically built in a closed network with limited remote access to the building operations. This was a reason to reduce exposing the remote attacks of EMS. Recently, EMS became a part of IoT system; hence cyber security became an essential task at the building commissioning time. A common commercial building automation tools for monitoring and policy editor use basic features based on some guidelines, such as *NESCOR* standard. ANASTACIA introduces the baseline for securely integrating several heterogeneous cyber physical system components, and providing intrusion detection and resiliency capability to the EMS.

ANASTACIA aims to detect uncommon behaviour in the BEMS and react and adapt the system, for instance enforcing security policy to isolate the compromised smart objects from the rest of the BMS system or improving the security between certain IoT devices or within devices in some networks.

3.2 Multi-access Edge Computing (MEC)

Nowadays, many companies have adopted the cloud technologies as growing strategy. Indeed, the cloud brings power, agility, and cost saving due to its computing and storage capacities. According to Thales Data Threat Report [Thales, 2017], Advanced Technology Edition, issued in conjunction with analyst firm 451 research, 93% of respondents will use sensitive data in an advanced technology (as cloud, SaaS, big data, IoT and container) environments this year. A majority of those respondents (69%) also believe their organizations are deploying these technologies ahead of having appropriate data security solutions in place and 88% believe network security very/extremely effective at protecting data. Moreover, security attacks as DDoS become a major issue in term of costs to the digital economy actors. Recently, a new cloud paradigm called Multi-access Edge Computing is emerging, pushed by ETSI [ETSI, 2015]. Multi-access Edge Computing (MEC) offers application developers and content providers, cloud-computing capabilities and an IT service environment at the edge of the network. This environment is characterized by ultra-low latency

and high bandwidth as well as real-time access to radio network information that can be leveraged by applications. The MEC needs to plan for the best computing facility placement to serve the requests and that is also able to online schedule virtual machine resources and request assignment to cloud facilities and to secure the different communication and to mitigate the security attacks. ANASTACIA aims to ensure that, the system can react to minimize different security attacks. ANASTACIA will assist administrators (end users) to provide an enforced network access policy and allow them to protect the exchanged data more over it of credentials. The administrators can use ANASTACIA to ensure that his system is safe from the attacks and to defense in case of security attacks. Indeed, by using ANASTACIA, end users, can detect an attack and send it to the right modules in order to stop the attacks by deploying the appropriate security appliances as demand in the right places based on SDN and NFV technologies.

In fact, the smart security cameras and IoTs can be used for a massive distributed denial-of-service (DDoS) as the attack that disrupted U.S. internet traffic on the October 21th 2016, where the attacks were made possible by the large number of unsecured internet-connected digital devices, such as home routers and surveillance cameras. Even though some of these devices are not powerful computers, they can generate massive amounts of bogus traffic, especially using a large numbers of IoT devices. The detection and mitigation of such kind of attacks need dynamic and agile features to accommodate to the attacks. Anastacia aims to fulfill such as needs by proposing a solution based on NFV and SDN approaches that bring remarkable benefits to provide on-demand security features in software-based networks. Moreover, the increased capabilities of Edge infrastructure can even augment the efficiency of the envisioned security solutions, by enabling prompt reactions near the IoT devices.

3.3 INTERNET OF THINGS (IOT)

The issue of security and privacy is heightened in IoT domains: as the connectivity of objects exponentially increases, so are the possibilities for hacking into the system. It is noted that IoT covers a huge scope of diverse markets and the needs of security and privacy vary depending on the types of services. In order to find general requirements from the user perspective, we focus on the common risks coming from the IoT communication patterns that apply to heterogeneous IoT services and applications.

Communication types in IoT systems include end-device to end-device (e.g., sensor node to sensor node, sensor node to actuator, etc.), end-device to gateway, gateway to central devices (e.g., cloud server, IoT platform servers, etc.), and/or central devices to application servers. The network communications for IoT services and applications naturally embed the traditional security and privacy risks, such as session hijacking, DDoS attack, denial service, IP spoofing, man-in-the-middle, etc. What brings more cautious on IoT in security and privacy is the vulnerability of IoT devices. It is well known that the low-powered sensor nodes and their communication protocols are much vulnerable on security attacks. In addition to it, privacy related data such as location info is often included for IoT services, which brings the needs of careful privacy design. The news on the Teddy bear hacking in the cyber security conference in at the World Forum in The Hague[2] on May 16, 2017 demonstrates the security weakness of IoT communication protocols, that 11 years old boy, Paul demonstrated his abilities by using his bear, which connected to the cloud via Wi-Fi and Bluetooth, to receive and transmit messages. He plugged a Raspberry Pi into his computer and scanned the conference hall for Bluetooth-connected devices. The other news in February of 2017 that police officers in England arrested a London suspect who allegedly hacked into home routers in 2016 over 1 million German households[3] also gives increasing alarms on IoT based services. We should pay attention that no security enabled home IoT devices are connected to Internet and any devices connected to the home routers can be hacked. The other example of showing vulnerability of IoT devices is the news that a

[2] https://securityintelligence.com/news/with-teddy-bear-bluetooth-hack-11-year-old-proves-iot-security-is-no-childs-play/
[3] http://www.news1130.com/2017/02/23/german-federal-police-say-british-hacker-arrested-in-london/

couple has been arrested by hacking Washington's CCTV days before President Trump's inauguration[4]. The news on hacking in IoT systems and devices are coming more often, which means that security and privacy alerts on IoT are increasing more and more by more devices are connected each other.

The other aspect to be considered related to IoT security and privacy is regulation related issues on policies to share privacy data among stakeholders. When IoT is integrated with robotics, these needs become more complicate and even include ethic issues. Thus, it is extremely important to build security and privacy system by design and also to provide users clear information on the security level of the system to be used and to notify users whether there is a risk on privacy data on using the system or services. ANASTACIA can fulfill such needs by designing and implementing holistic solutions enabling trust and security by-design for cyber physical systems (CPS) based on IoT and cloud architectures. Especially, it also includes dynamic security and privacy seal providing users certification level of the system and information on privacy data.

[4] http://www.telegraph.co.uk/news/2017/02/05/two-arrested-london-hacking-us-cctv-systems-days-president-trumps/

4 BUSINESS PERSPECTIVE ANALYSIS

Industrial Control Systems (ICS) play an important role in the monitoring and control of physical and chemical processes. ICS is a general term that encompasses several types of control systems, used in EMS, industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems, and other smaller control system configurations such as programmable logic controllers (PLC), often found in the industrial sectors and critical infrastructures. Automatic control of electrical/thermal components in buildings has become a necessary task for ICSs, in order to achieve optimal performance. In this context, the ICS is often called an energy management system (EMS). Nowadays, EMS industry looking for developing a secure EMS that detects attacks and maintains the physical system in a safe state, during and after the detected attack.

On the other side, Internet of Things applications have opened a big investment market to offer innovative services that enrich the quality of life. For example, it has become common to have systems that collect data related with the traffic in huge cities, manage the energy and/or water system of a building and even monitor and control systems that maintain the security of the habitants of a whole country. These types of systems usually handle sensitive data and make decisions relying blindly on the quality of them. Therefore, the security of the whole platforms here described becomes a crucial topic when developing such technologies. Although the market already provides the technologies that implement the underlying platform, the proposition of a secure-by-design approach is still missing.

The ANASTACIA project aims tackling this lack of offer by providing the market with a complete set of tools and methodologies that cope with these challenges by:

- Proposing a secure-by-design modelling and developing approach,
- Developing a Cyber-physical network (CPS) managed by software defined network (SDN) techniques,
- Providing a set of monitoring and reaction tools that implement a security framework tailored for CPS and SDN,
- Defining a security and privacy seal used to guarantee the security of the monitored platform.

The set of tools designed aims to provide the market with innovative technologies tailored for the specific use cases of the ANASTACIA project. However, the project will also prioritize the usage of open standards and modular approaches, facilitating the adaptation of the ANASTACIA framework to other use cases and technologies.

The described set of technologies and methodologies will enhance the market by bringing a cost-effective way to ensure the security of cyber physical networks. The ANASTACIA project will enlarge the value proposition of the market by bringing a novel and complete solution to implement secure cyber physical networks, which is mainly composed by a set of tools solving each one a part of the whole problematic. For example, the market proposition is based on Firewalls and Intrusion Detection Systems that are able to detect some attacks, although they are designed for specific endpoints and network architectures. In addition, these tools do not support automatic reaction, leaving the decision and implementation of the countermeasure to be implemented manually but the system administrator. This fact makes the deployments of such systems a big challenge when trying to adapt them to cyber physical networks. The proposition of a complete approach and its security certification is part of the main value proposition of the expected results.

In this sense, this proposal will not only attract actual enterprises that use IoT-based cyber physical network, but also new potential customers that will rely on the ANASTACIA approach to enhance their systems with the automatic security enforcement mechanisms provided by the project. These enterprises include, but are not limited to governments, energy and water companies, real estate and transportation companies. At the same time, these companies might be interested in investing in the proposed

technologies, which will allow them to adapt the results of the project to their requirements, and deploy it in new environments.

In summary, ANASTACIA points its principal business area to the adoption of the developed technologies and methodologies into existing SDN- and NFV-based IoT networks. At the same time, the development of a Security seal will open the business opportunities of certifying already-existing IoT deployments. In both areas, the ANASTACIA partners look forward to exploiting the project's results by enhancing their tools to tackle the use in the frame of the project, but also adapting them to new use cases, leading to new business opportunities.

5 TECHNICAL PERSPECTIVE ANALYSIS

In this section of the document, we report the technical perspective analysis accomplished during the development of the project. The ANASTACIA project relies on policy-based network and security management to deal with cyber-attacks in CPS-IoT scenarios through SDN and NFV. We will now focus on the analysis of current security policy model proposals and solutions under consideration, hence discussing software-based network security enablers. Finally, we focus on new security and privacy threats in IoT.

5.1 SECURITY POLICY MODEL PROPOSALS UNDER CONSIDERATION

5.1.1 xCIM-SDL/SPL

Common Information Model (CIM)[5] is the main standard that provides a common definition of management-related information independent of any specification. The model defines concepts for authorization, authentication, delegation, filtering, and obligation policies. However, for an information model to be useful, it has to be mapped into some specification and for our propose CIM models are not suitable by itself, due to the huge amount of classes which is compound, so xCIM [Bernal] model is based on CIM, but including only the relevant classes of the model as well as some extended classes.

xCIM Security Policy Language (xCIM-SPL) allows to the user the definition of security policies in order to establish the desired security behaviour of the system, using a friendly high level language nearly to the spoken English, whereas xCIM System Description Language (xCIM-SDL) is a submodel that allow to describe the system in a medium level abstraction representation. Both are based on XML and were applied on the scope of POSITIF[6] and DESEREC[7] European projects.

Currently, xCIM-SPL supports filtering, authentication, authorization, channel protection and operational policies policy types, but the language is easily extensible. Composed of an XML schema for each type of security policy, the xCIM-SPL is composed of five independent XML schemas.

The link between xCIM-SPL and SDL elements is done using the internal format. The internal format is a low level language for formal modelling designed for developers. Since both SPL and SDL instances are defined in internal format, this link is directly achieved using the internal format. To build automatically the XML schema from any CIM version authors designed an automatic transformation.

[5] http://www.dmtf.org/standards/cim
[6] http://cordis.europa.eu/project/rcn/75115_en.html
[7] http://www.deserec.eu

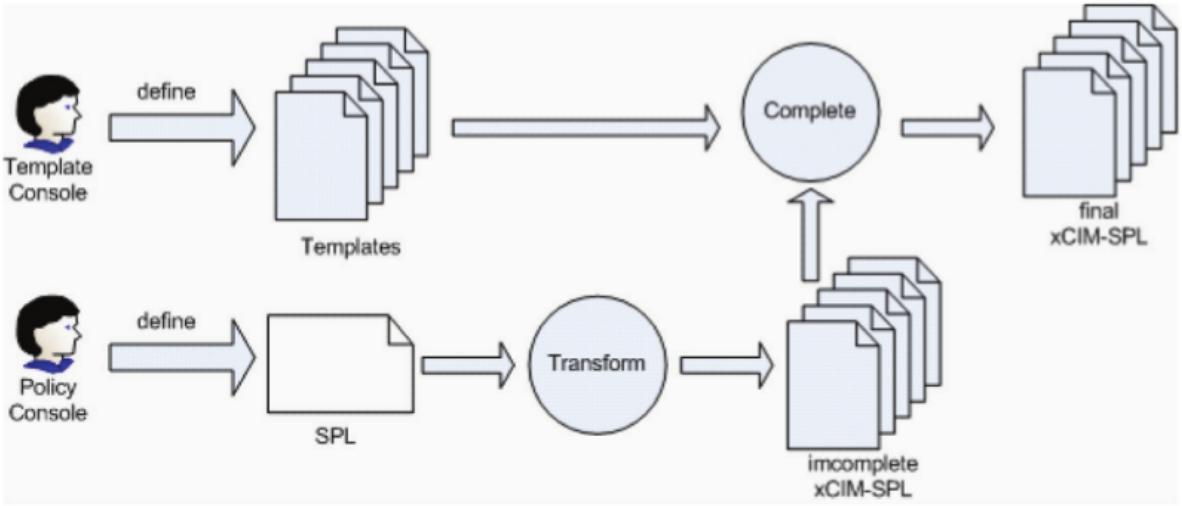

Figure 4: SPL to xCIM translation process

The refinement consists in a translation from the high-level specification to low-level rules specified by a language based CIM-Policy Information Model (i.e. xCIM-SPL or internal format). The translation process is based on the direct transformation the SPL elements to xCIM-SPL elements. But due to lack of information provided by the natural human concepts, the authors use templates for fill it, and in order to ease the definition, transformation and manipulation of security policies also provide a policy console.

5.1.2 SECURED – HSPL/MSPL

High-level Security Policy Language (HSPL) and Medium-level Security Policy Language (MSPL) [Vallini] are two policy languages defined within the European SECURED[8] project in order to specify security policies. HSPL is the policy language suitable for expressing the general protection requirements of typical non-technical end-users, such as “do not permit access to illegal content” or “block access to peer-to-peer networks”, whereas that MSPL is an abstract language with statements related to the typical actions performed by various security controls but expressed independent of the final devices, it means, expresses specific configurations by technically-savvy users in a device-independent format, such as “deny *.sex”, “deny src 192.168”, or “inspect image/* for malware”.

Both policy languages are based on XML and are focused on the capability concept. A capability denotes any kind of security functionality that can be provided by a Personal Security Application (PSA). A PSA implements some security controls, generally, by a software module, e.g. filtering, logging or authentication. Specifically, the model includes capabilities like authorization, authentication, data protection and general security.

Simplified HSPL Example

```
<hspl_list>
	<hspl subject='SensorA' id='HSPL0'>
		<action>no_authorise_access</action>
		<objectH>Internet_traffic</objectH>
	</hspl>
</hspl_list>
```

[8] http://www.secured-fp7.eu

MSPL is defined by a meta-model that specifies the main concepts (like policies, rules, conditions, and actions), and it is organized by capabilities. In this context, capabilities are defined as basic features that can be configured to enforce a security policy (e.g. channel protection, filtering, anti-virus, parental control…).

Simplified MSPL Example

```
<ITResource ID="MSPL_f9b27422-15b3-4bb5-ad21-3e08af5b1a1c"...>
    <configuration xsi:type="RuleSetConfiguration"...>
        <capability>
            <Name>Filtering_L4</Name>
        </capability>
        <defaultAction xsi:type="FilteringAction">
            <FilteringActionType>ALLOW</FilteringActionType>
        </defaultAction>
        <configurationRule>
            <configurationRuleAction xsi:type="FilteringAction">
                <FilteringActionType>DENY</FilteringActionType>
            </configurationRuleAction>
            <configurationCondition
                xsi:type="FilteringConfigurationCondition">
                <packetFilterCondition>
                    <SourceAddress>10.0.0.1,</SourceAddress>
                </packetFilterCondition>
            </configurationCondition>
            <Name>Rule0</Name>
        </configurationRule>
        <resolutionStrategy xsi:type="FMR"/>
        <Name>MSPL_f9b27422-15b3-4bb5-ad21-3e08af5b1a1c</Name>
    </configuration>
</ITResource>
```

Finally, MSPL policies are translated to a lower level tasks or configurations, it means, the policies are refined to a specific security configuration or task for a specific PSA. In order to support a wide set of low-level security controls is possible to develop different refinement plugins for each kind of technologies, e.g. NetFilter/iptables, SDN, etc.

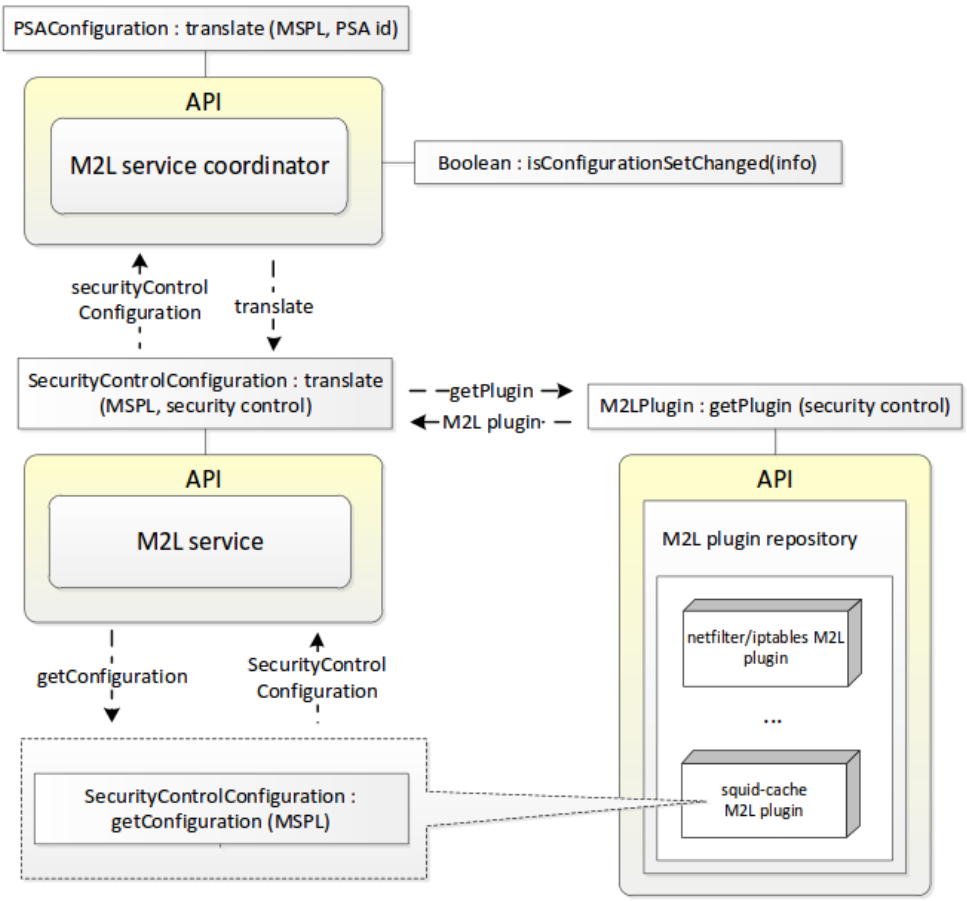

Figure 5:Medium to Low refinement process

Figure 5 shows workflow where a coordinator is requesting a translation from a MSPL policy to a lower security control configuration. In this case, a lower level service request to a plugin repository the plugin that is capable to translate the MSPL sentences into a specific security control configurations or tasks for a specific security control, e.g. iptables, NetFilter, etc. Once the service receives the suitable plugin, it invokes the method in charge to make the translation.

5.1.3 I2NSF Information Model of Network Security Functions Capabilities

I2NSF Information Model of Network Security Functions Capabilities from IETF [Xia, 2017] provides a definition for a model of security capabilities for automatic management of Network Security Functions (NSFs), understanding capabilities like a set of available features in a managed entity. This model provides standard interfaces in order to obtain the required NSF at a given time, and the criteria to select a specific NSF is independent to the vendor, relying instead on the capabilities. Furthermore, when an unknown threat (e.g., zero-day exploits, unknown malware, and APTs) is reported by a network security device, new capabilities may be created, and/or existing capabilities may be updated. These new capabilities may be sent and stored in a centralized repository, or stored separately in a local repository. In either cases, a standard interface is needed during this automated update process.

As can be seen on Figure 6, there are two relevant types of Interfaces to Network Security Functions (I2NSF):

- Interface between I2NSF clients and a security controller.
- Interface between NSFs.

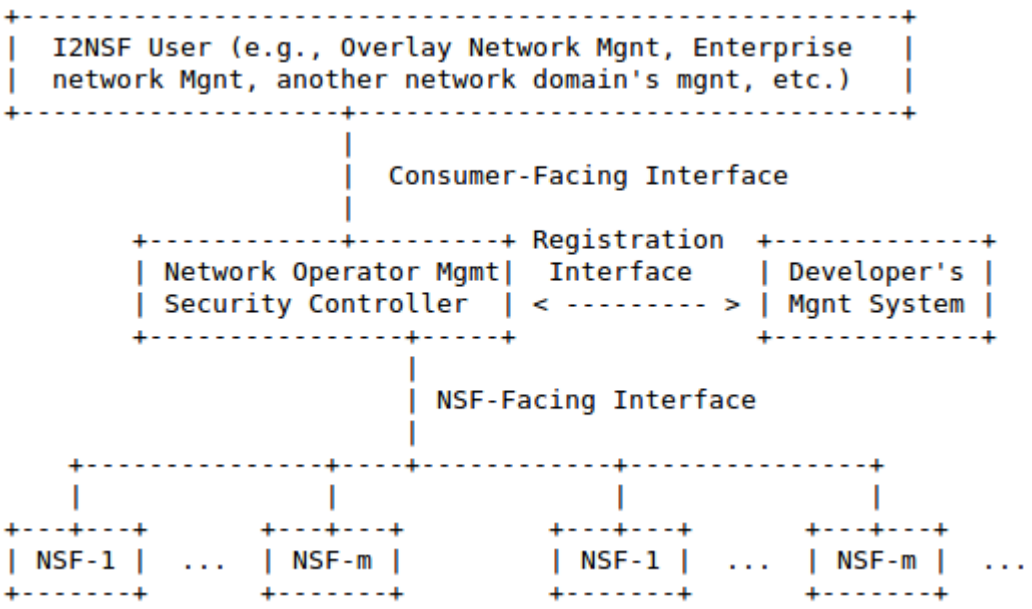

Figure 6: I2NSF Interfaces

In defining the capabilities of a NSF, it is used the "Event-Condition-Action" (ECA) policy rule set model:

- An Event is defined as any important occurrence in time of a change in the system being managed, and/or in the environment of the system being managed.
- A Condition is a set of attributes, features, and/or values that are to be compared with a set of known attributes, features, and/or values in order to make a decision.
- NSFs provide security functions by executing several Actions.

The I2NSF capability interface is in charge of controlling and managing the NSFs by means of the information about the capabilities each NSF owns. The capability interface is used for advertising, creating, selecting and managing a set of specific security capabilities independent of the type and vendor of device that contains the NSF.

Initially, there are three common categories of capabilities i.e. network security, content security and attack mitigation. Each category contains sub-models that provides more specific policy rules like authentication, accounting, authorization or traffic inspection rules.

5.1.4 Policy Models Relationship

The below Figure 7 shows the relationship between the aforementioned proposals. As can be seen, HSPL/MSPL extends and improves the idea exposed on xCIM-SPL/SDL, and I2NSF IETF group reuses and extends the concept on I2SNF Framework.

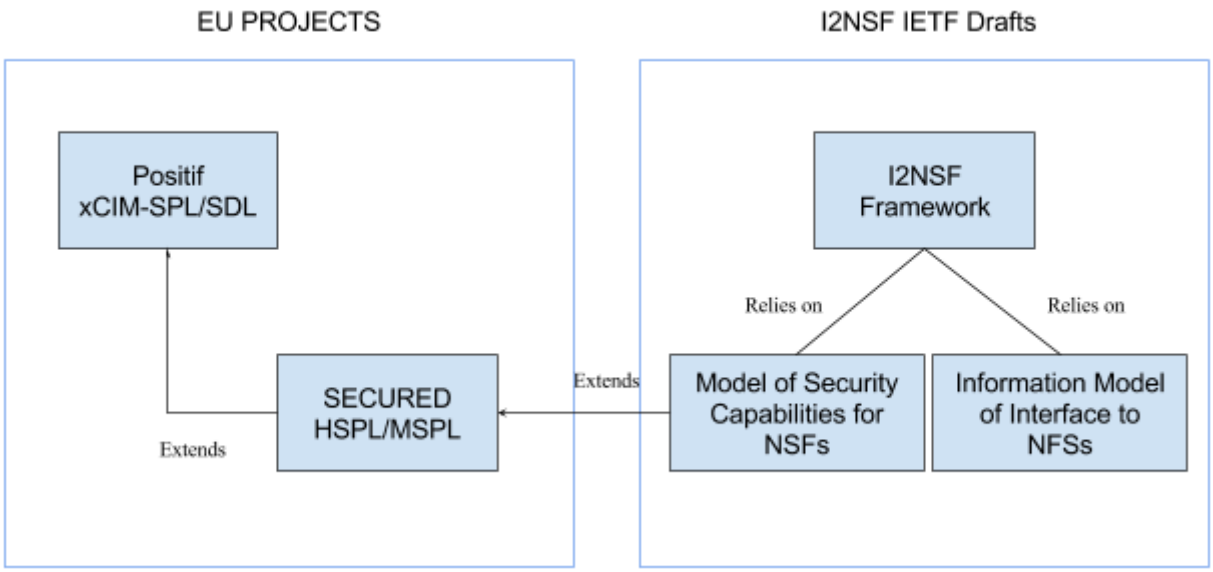

Figure 7: Policy Models Relationship

Framework for Interface to Network Security is described on draft draft-ietf-i2nsf-framework-04[9] and defines a reference model for I2NSF. A model of a Security Capabilities is presented on draft draft-baspez-i2nsf-capabilities-00[10], whereas draft-xia-i2nsf-capability-interface-im-06[11] is focused on the capability interface of NSFs and proposes its information model for managing the various network security functions. The last two drafts are merged on draft-xibassnez-i2nsf-capability-00[12], and there is a recent update on draft-xibassnez-i2nsf-capability-01[13].

5.2 SECURITY POLICIES SOLUTIONS UNDER CONSIDERATION

The OpenDaylight Network Intent Composition[14] project will enable the controller to manage and direct network services and network resources based on describing the "Intent" for network behaviours and network policies. It means, is an interface that allows clients to express a desired state in an implementation-neutral form that will be enforced via modification of available resources under the control of the OpenDaylight system.

[9] https://tools.ietf.org/html/draft-ietf-i2nsf-framework-04
[10] https://tools.ietf.org/html/draft-baspez-i2nsf-capabilities-00
[11] https://tools.ietf.org/html/draft-xia-i2nsf-capability-interface-im-06
[12] https://tools.ietf.org/html/draft-xibassnez-i2nsf-capability-00
[13] https://tools.ietf.org/html/draft-xibassnez-i2nsf-capability-01
[14] https://wiki.opendaylight.org/view/Network_Intent_Composition:Main

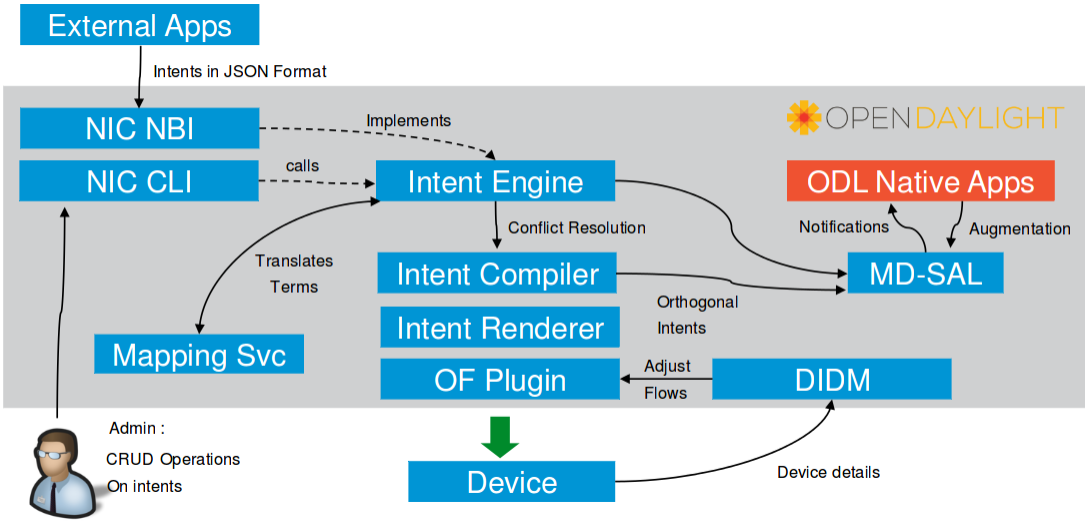

Figure 8: ODL intent workflow

As can be seen in Figure 8, intents are described to the controller through a new NorthBound Interface which provides generalized and abstracted policy semantics instead of Openflow-like flow rules. The policies are expressed generally on XML or JSON, and the component that transforms the intent to the implementation is typically referred to as a renderer.

On the other hand, ONOS also has its own intent framework. The ONOS Intent Framework[15] is a subsystem that allows applications to specify their network control desires in form of policy rather than mechanism. Authors refers to these policy-based directives as intents. These intents can be translated via intent compilation into installable intents which results on some changes over the environment. ONOS provides a set of built-in intents, but the framework is extensible in order to allow developers to add its own dynamically.

Beyond the SDN controllers, Open Stack Group Based Policy[16] introduces a concept of a group that represents a collection of network endpoints and fully describes their properties. Everything in the same group must be treated the same way (that is it has the same policy). GBP introduces also a rule sets to describe secure connectivity between Groups as is illustrated on Figure 9. Rule sets may imply switching or routing behaviours, but they offer a simple way to describe how sets of machines can communicate in non-networking terms. Critically, they are also reusable. The same rule set can be used for different combinations of Groups. Automation and security are much easier through GBP. By simply becoming a member of a group, a virtual machine inherits all of its policies, allowing developers to easily automate scaling up and down. In fact, it was designed to make advanced capabilities such as service chaining extremely easy to use. As GBP has progressed in OpenStack, a corresponding project has been developed in the ODL community to build an open source network overlay solution using ODL and Open vSwitch (OVS). The GBP project can naturally support OpenDaylight in this configuration and allow it to act as a network controller through its existing southbound interface.

[15] https://wiki.onosproject.org/display/ONOS/Intent+Framework
[16] https://wiki.openstack.org/wiki/GroupBasedPolicy

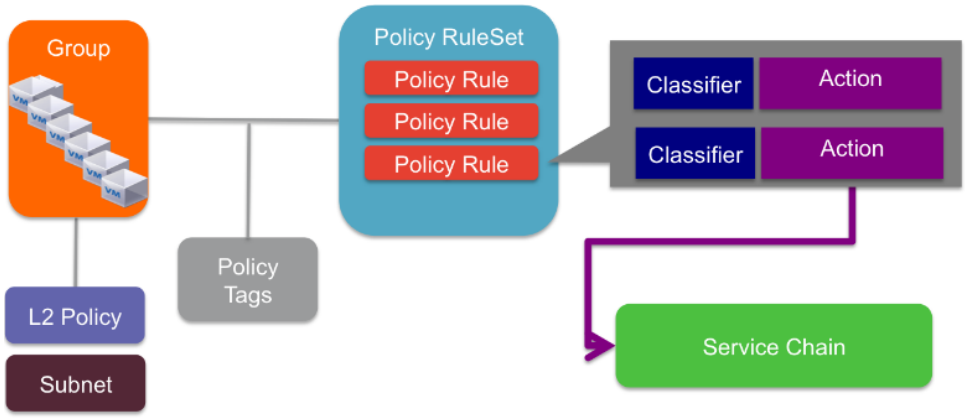

Figure 9: OS Group Based Policy

The OpenDaylight Group Based Policy[17] project defines and implements an intent system, allowing users to express network configuration in a declarative versus imperative way. GBP offers an intent based interface, accessed via the GUI called UX, via the REST API or directly from a domain-specific-language such as Neutron through a mapping interface. This integration will allow perform operations not currently available in OpenStack like the use of Service Function Chaining. The major benefit of this architecture is that the mapping of the domain-specific-language is completely separate and independent of the underlying renderer implementation, it means, when another renderer is added, for instance, NetConf, the same policy can now be leveraged across NetConf devices simultaneously.

Backing again to OpenStack, Congress[18] provides a mechanism to allow OpenStack clients to define policy to be applied across all OpenStack components, not only networking related. It is a cloud service whose sole responsibility is policy enforcement which uses the Neutron Group-based policy in order to provide a high-level abstraction for defining network connectivity between groups of endpoints. The policy language supported by Congress must be general-purpose and declarative. Actually, OpenStack Congress is using Datalog as policy language.

5.3 Overview of Software-based Network Security Enablers

The ANASTACIA project aims at exploring the opportunities that Software Defined Networking and Network Function Virtualization offer in coping with security threats against IoT services. In this vein, the efficient orchestration of software-based security enablers plays a key role to meet the desired policy-driven security requirements. In the following Sections, we present these emerging network solutions, especially highlighting their features and benefits towards the provisioning of advanced security mechanisms.

5.3.1 Overview of Software Defined Networking

Software Defined Networking (SDN) is a network architecture which decouples the control and forwarding functions, introducing enhanced network programmability. Accounting for the separation of control and data planes, network control can be done separately, without affecting data flows. In this way, network intelligence is provided by a centralized controller and the complexity of the underlying switching devices is notably reduced in comparison with traditional networks. The SDN paradigm offers a simpler programmable network environment and a higher level of flexibility for external applications to define the network behaviour.

[17] https://wiki.opendaylight.org/view/Group_Based_Policy_(GBP)
[18] https://wiki.openstack.org/wiki/Congress

Open Networking Foundation (ONF)[19], a non-profit consortium dedicated to development, standardization, and commercialization of SDN, has suggested a reference model for SDN networks, as sketched in Figure 10. This architecture includes three layers:

- The **data plane** includes network elements (e.g., switches, routers, etc.) which are responsible for processing packets based on the rules provided by a controller, and for collecting network status, such as network topology and traffic statistics.
- The **control plane** bridges the application plane and the data plane, translating applications' requirements into appropriate forwarding rules to be enforced over the underlying network switches. To this aim, the south-bound interface allows the SDN controller to access functions provided by the switching devices. These functions may include reporting network status and managing packet forwarding rules. On the other hand, the north-bound interface provides service access points in various forms, e.g., Application Programming Interfaces (APIs), so that SDN applications can communicate their network requirements to the SDN controller. Also, via the northbound APIs, the SDN applications can access network status information reported from switching devices, modify network behaviour accordingly, and request new packet forwarding rules to switching devices.
- The **application plane** refers to the SDN applications developed to implement specific user requirements. Through the interfaces provided by the controller, SDN applications, such as dynamic access control and load balancing, may have dynamic and granular access of network resources, and define traffic flows at the data plane.

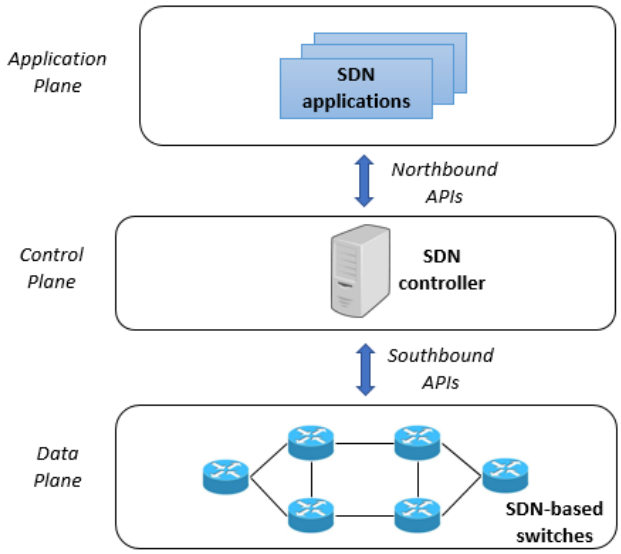

Figure 10: SDN reference architecture

Two main open-source projects are leading the adoption of SDN in a broad range of environments. Open Network Operating System (ONOS)[20] is a distributed and modular SDN controller specifically designed for service providers. The main goals behind its development are high availability, scalability, and performance. The network configuration can be communicated to the controller through its northbound APIs as intents, which are enforced in the underlying network through the southbound APIs using the OpenFlow protocol. Open DayLight} (ODL)[21] is an open source SDN controller supported by the Linux foundation. Similar to ONOS, it is modular and supports the OpenFlow protocol for southbound communications, as well as other standard protocols defined by the IETF, such as NETCONF. ODL employs a model-driven approach to describe the network, the functions to be performed on it and the resulting state or status achieved.

[19] Open Networking Foundation, https://www.opennetworking.org/sdn-resources/sdn-definition
[20] ONOS project, http://onosproject.org/
[21] Open DayLight, https://www.opendaylight.org/

5.3.1.1 SDN features for enabling security mechanisms

The use of software-defined networking is gaining high momentum also in the security research communities [Ali, 2015]. In this Section, we provide an overview of the major SDN features which can be explored to provide advanced security countermeasures for IoT systems within the ANASTACIA project.

Dynamic Flow Control: By leveraging the decoupling of control and data planes, a network application can manage network flows dynamically. Indeed, when an SDN switch does not have a flow rule to process a specific packet, a relevant request is forwarded to the controller which can decide the relevant packet processing based on specific application policies. This feature can enable a dynamic access control function, which is commonly implemented to protect a network according to the specified privileges and policies.

Traffic Isolation: SDN can be exploited to enable forwarding of different network traffics over the same physical network infrastructure, while guaranteeing the desired level of isolation [Sherwood, 2009]. This feature can drastically limit the propagation and damages of security attacks between different network domains. Furthermore, it can be used to separate malicious (or suspicious) network flows dynamically. In this vein, SDN-based separation solutions can offer different level of network abstractions, so to appropriately separate network traffics and provide network views according to desired security properties.

Network-Wide Visibility with Centralized Control: In SDN, all data planes are managed by a centralized controller which is in charge of flow rule configuration. In addition, through the control plane, network status information can be collected from each data plane by sending statistics query messages. Therefore, a network application running on the control plane can have updated status of relevant data plane and flow request messages through the northbound APIs. In this way, SDN can ease the network-wide monitoring and the detection/defence of network-wide attacks. For example, the network administrator can implement anomaly analysis to identify network-wide attacks by monitoring the network state changes. Moreover, network resource can be timely reorganized to mitigate large-scale network security vectors.

Network Programmability: Since data forwarding in an SDN network can be controlled by a network application program, SDN provides an enhanced flexibility to enable new network functions and to extend network functionalities. To empower this feature, several network programming languages have been proposed so far [Trois, 2016], boosting the development of new SDN-based network applications.

5.3.2 Overview of Network Function Virtualization

The deployment of virtualized network services provides remarkable benefits in terms of increased flexibility, improved capital efficiency, and enhanced operational efficiencies in Telco networks [Taleb, 2014]. ETSI ISG NFV has designed a high-level functional architectural framework for the management of virtualized network functions [ETSI-NFV, 2014], which includes three layers, as illustrated in Figure 11:

- Network Functions Virtualization Infrastructure (NFVI) block
- Virtualized Network Function (VNF) block
- Management and Orchestration (MANO) block

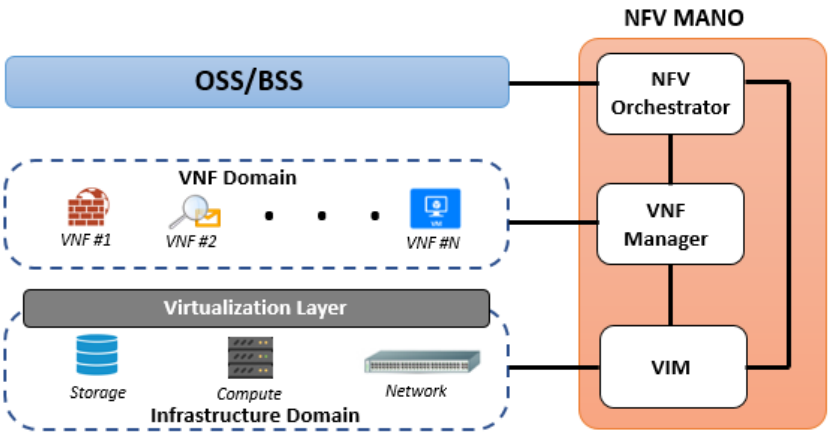

Figure 11: ETSI NFV reference architecture

Network Functions Virtualization Infrastructure (NFVI) block: This block comprises the hardware resources providing necessary processing, storage, and network capabilities, as well as the virtualization software components, to create the virtualization environment.

Virtualized Network Function (VNF) block: The VNF block refers to the virtual network functions (VNFs) which are executed leveraging the virtualized resources offered by the underlying NFVI.

Management and Orchestration (MANO) block: MANO is defined as a separate block in the architecture, which interacts with both the NFVI and the VNF blocks. The ETSI NFV framework delegates to the MANO layer the management of all the resources in the infrastructure layer for the efficient deployment of the VNFs. The MANO main components are:

- Virtualized Infrastructure Manager (VIM): VIM manages the virtualization layer and controls how the hardware resources are used in NFVI block. VIM is therefore responsible for the control of NFVI resources including the creation, maintenance and management of virtual machines (VMs). It also operates with other management functional blocks to determine the service requirements and then manage the infrastructure resources to fulfil them.
- VNF Manager (VNFM): VNFM is responsible for the control of VNFs lifecycle, including the creation, configuration, maintenance, performance, and security management of VNF instances.
- NFV Orchestrator (NFVO): NFVO has a central role in the framework by covering both resource and service orchestration. To this aim, the NFVO works with the VIM to provide the resources necessary for hosting VNFs. Furthermore, the NFVO is in charge of interacting with the VNFM to manage the configuration of relevant VNF.

Furthermore, the ETSI NFV ISG has specified several information elements to efficiently manage the on-boarding and lifecycle of Network Service (NS) and relevant VNFs. A NS can be considered as a forwarding graph of Network Functions interconnected by supporting network infrastructure. In the following we provide a brief description of the main ETSI NFV information models [ETSI-NFV-MANO, 2014].

A *VNF Descriptor (VNFD)* is a template which describes a VNF in terms of its deployment and operational behaviour requirements. It is primarily used by the VNFM in the process of VNF instantiation and lifecycle management of a VNF instance. The VNFD also contains connectivity, interface and KPIs requirements that can be used by NFV MANO functional blocks to establish appropriate Virtual Links (VLs) within the NFVI between its VNF Component instances, or between a VNF instance and the endpoint interface to the other Network Functions.

A *Virtual Link Descriptor (VLD)* is a deployment template which describes the resource requirements that are needed for a link between VNFs, Physical Network Functions (PNFs) and endpoints of the NS, which could be met by various link options that are available in the NFVI.

At the highest level of the ETSI NFV information models, the *Network Service Descriptor (NSD)* is used by the NFVO to instantiate a NS, which can be composed by one or more VNFs, PNFs, and VLs. Furthermore, several VNF Forwarding Graphs can be defined to steer traffic among different network forwarding paths, e.g., to meet specific QoS requirements. Therefore, a NSD is a deployment template for a NS which references all other descriptors required for the components included in the NS.

To boost the adoption of the NFV paradigm, several open-source projects have been developed recently. In the following we list the main initiatives:

OpenBaton[22], developed by Fraunhofer FOKUS and TU Berlin, is an open source NFV platform whose architecture is ETSI MANO compliant. It ensures the development of virtual network infrastructures by porting and further adapting network functions to the specific cloud environment. The OpenBaton project integrates an NFV Orchestrator to coordinate network services deployment, and a generic VNF Manager that can be replaced by either Juju or customized VNFMs using a vnfm-sdk. The life-cycle of deployed VNFs can be managed through an Element Management System. OpenBaton also enables multi-tenancy between different operators.

Open Source Mano (OSM)[23] is an ETSI-hosted project that aims to provide end-to-end service provisioning and orchestration through a Network Service Orchestrator. The framework also includes a Resource Orchestrator responsible for processing the resource allocation requirements of each VNF, based on the corresponding descriptor. OSM can also integrate multiple VIMs for resource provisioning, and SDN controllers for network management.

Open Network Automation Platform (ONAP)[24] is a recent project derived from the merging of two different open-source NFV platforms, i.e., ECOMP (Enhanced Control, Orchestration, Management and Policy) and Open-O. It aims at creating a harmonized and comprehensive framework for real-time, policy-driven software automation of VNFs. It expands the scope of ETSI MANO compliant including further software components and providing support for efficient utilization of network resources, elasticity, security, and reliability.

5.3.2.1 NFV features for enabling security mechanisms

The NFV paradigm offers promising features to increase the network capabilities offered by Telco providers and to provide the opportunities to faster develop and deploy new network services. Different opportunities for enabling and efficiently orchestrating security enablers can also be envisaged by exploiting the NFV paradigm, whose key features are discussed in the following.

Decoupling software from hardware: the basic principle of NFV deals with the opportunities to use commodity servers for deploying virtualized network functions. In this way, notable reduction of dedicated hardware can be achieved. This aspect can be extremely significant also in the network security domain, where hardware-based firewall, DPIs, etc. can be replaced by software-based instances.

On-demand scalability: by exploiting the dynamic instantiation of VNFs, network administrator can achieve a higher level of scalability and allow finer granularity. In this way, virtual security network functions can be scaled up/down according to the current workload, thus ensuring the required performance.

Flexible network service provisioning: The software-based deployment allows for increased efficiency in the deployment of services over a shared physical infrastructure. Furthermore, different components can be dynamically integrated along the forwarding paths. This can enable the creation of appropriate security service chains where user traffic is appropriately processed according to security policies. Also, security operators can leverage software-based functions deployment to timely mitigate detected security attacks.

[22] Open Baton project, http://openbaton.github.io
[23] Open Source Mano project, https://osm.etsi.org
[24] Open Network Automation Platform project, https://www.onap.org

The NFV paradigm fully embraces the cloud delivery models of on-demand service provisioning, thus supporting the concept of Security-as-a-Service. In this vein, the Cloud Security Alliance (CSA)[25] has defined guidelines for cloud-delivered defence solutions, to assist enterprises and end-user to widely adopt this security paradigm shift. The NFV approach presents remarkable advantages with respect to the hosting in remote cloud data centers, since the virtualized security functions can be deployed along the forwarding path, avoiding inefficient traffic detouring. Furthermore, the provisioning of security functions towards the edge of the network can better scale with the expected huge amount of traffic generated by IoT devices.

5.4 NEW SECURITY AND PRIVACY THREATS IN IOT

With the number of IoT devices increasing, customers accessing to this technology are also increasing, leveraged by the reduction of prices and the increase on the number of functionalities. Furthermore, IoT devices are becoming a critical part of Cyber Physical Systems which are the core of many critical infrastructures.

This section analyses the current context regarding the security and privacy threats currently appearing in IoT/CPS. It is worth noticing that there are important differences between the traditional IT domain and the current IoT/CPS context. These differences really impact on the type of events threatening these platforms and how they are managed.

The main differences derive from the dynamic and changing character of IoT/CPS platforms, with a large number of devices connecting and disconnecting, installed and uninstalled in a short period of time. This is especially critical for activities such as patching and updating, which are difficult (and costly) to address in such changing environments. Not to mention compliance requirements that new updates might need to fulfil, in order to avoid violations of certifications procedures that these systems, if running on a critical environment, need to comply.

Closely related to the dynamicity of IoT/CPS platforms is the large amount of legacy systems running in these platforms. It is common that many devices from different vendors use different protocols and have different capabilities. Sometimes they are providing just analogue signals that have to be transformed into digital information in order to be used within the platform. This is an issue that has a high impact on the security of an IoT /CPS platform, as many legacy systems require tailored implementations of certain security mechanisms. For other devices, due to resource limitations, those security mechanisms are not even possible.

Another aspect that is inherent to IoT/CPS is the real-time capabilities that, very often, these systems require. This impacts on the way that security events and potential threats are managed, as availability might become a paramount aspect to consider, especially for very critical domains.

The aforementioned distinctive features are exploited by malicious parties to design attacks, but, who are these malicious parties and what are their motivations? Authors in [Cardenas09] classify potential attackers into four main groups: (1) cybercriminals, which aim is to target any unprotected system, with no specific purpose, but whose attacks might cause negative side effects. (2) Disgruntled employees, or simply careless ones, installing malware from the inside of the system. These insiders' attacks are very difficult to manage, as the attacker has direct access to the computer and networks, even if the network is physically disconnected from the public Internet. (3) Terrorists, activists and organized criminal groups, which have deep knowledge of systems and are able to exploit even unknown vulnerabilities. Very often these attackers are motivated by economic interests, using them for extortions or simply for public discredit. (4) Nation states, mainly focused on cyber espionage.

The following subsections analyse the context of threats in IoT/CPS from three perspectives:

[25] Cloud Security Alliance, https://cloudsecurityalliance.org

Analysis of threats: what are threats and what are the dimensions that need to be considered when analysing them.

Analysis of cyber-attacks: what is the lifecycle of an attack, this is, the identification of the phases that any attack follows when breaking into a system.

Security objectives: what are the objectives that any security protection policy has to consider when dealing with the protection against potential threats and their corresponding attacks.

The current analysis of threats management in IoT/CPS concludes with the identification of the most paramount attacks and threats and a classification of countermeasures.

5.4.1 Cyber Threat Analysis

According to the InfoSec Institute [Kost14], a threat could be *anything that leads to interruption, meddling or destruction of any valuable service or item existing in the firm's repertoire*. Threat analysis is essential to combat cyber-attacks. The analysis of the information, internal and external, associated to a potential threat represents the difference between reacting to attacks and preventing attacks, thus reducing its impact within a system.

Threat analysis evaluates four dimensions associated to potential threats:

1. Scope, which is the collection of items (devices, information, premises, and services) that a threat can target, and thus, can be potentially compromised.
2. Data collection, which is the ability to gather cyber threat information used by threats, such as vulnerabilities, list of open ports, list of emails or IP addresses of a system.
3. Risk analysis, in order to determine the level of exposure to a threat. This is done by evaluating the current mechanisms that an IoT/CPS platform has to neutralize threats in terms of availability, confidentiality and integrity.
4. Mitigation and anticipation, derived from the outcomes of phases (1), (2) and (3). This phase would be capable of designing mitigation measures and prevent similar attacks in the future.

It is worth noticing that, despite the fact that any IoT/CPS platform might be subject to be attacked in many ways, the risk of suffering a successful cyber-attack is higher when three aspects converge (see Figure 12):

- System Susceptibility. Not all systems are vulnerable to be attacked. In general, updated systems are less vulnerable that systems with outdated software installed in their devices. As mentioned before, this is a problem in IoT/CPS platforms, with a large number of many different devices running different operative systems or built with different technologies. Additionally, not all systems are interesting for attackers. Only those targets that might return the attacker any type of value are worth the effort of exploiting known vulnerabilities (even more for the effort of discovering and exploiting zero-day vulnerabilities).
- Threat accessibility. Not all systems are accessible to be attacked. Devices physically disconnected from the public internet are less vulnerable to cyber-attacks, while devices physically protected are less vulnerable to tampering attacks.
- Threat capability. The existence of known techniques or tools to exploit vulnerabilities makes it easier for attackers to succeed.

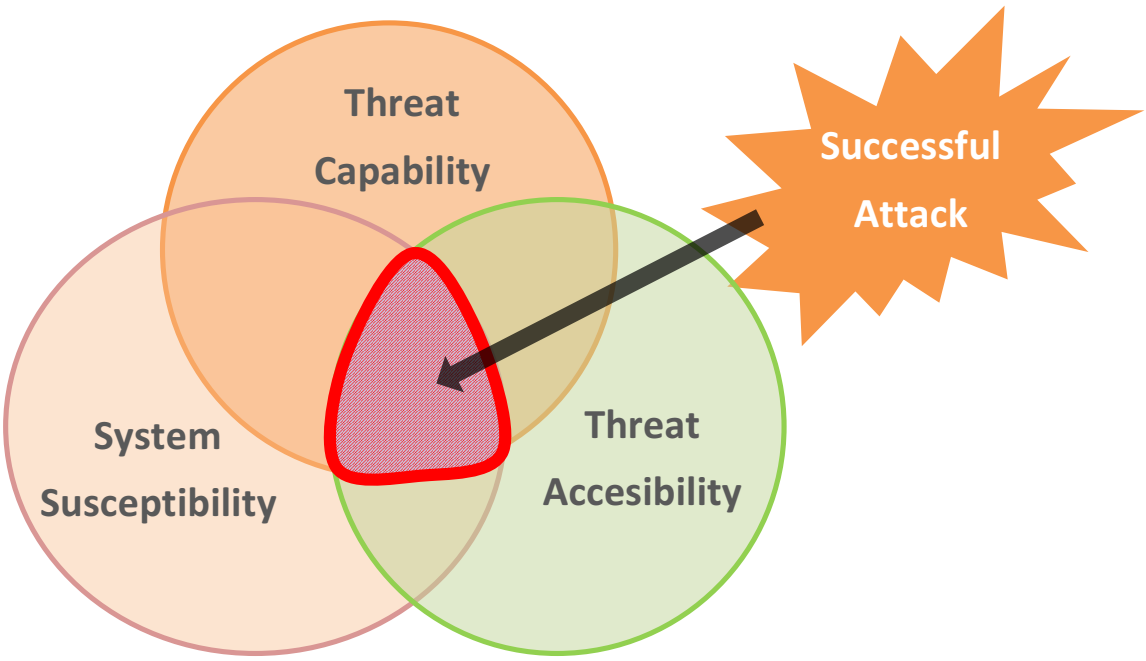

Figure 12: Dimensions of a successful attack

Therefore, when these three dimensions converge at the same time, the likelihood of being attacked is high, and therefore the system/platform is clearly compromised.

5.4.2 Lifecycle of Cyber Attacks

The previous threat analysis can be detailed in a set of stages that typically characterize the lifecycle of a cyberattack [Sage17] [LECC]:

- Initial reconnaissance: an attacker will study the scope of his/her attack by evaluating the available defences of a system and its potential vulnerabilities, either logical (i.e., software zero-day vulnerabilities), physical (i.e., direct access to a temperature sensor) or human (i.e., unsatisfied employee).
- Initial compromise: an attacker is able to gain entry in some system/platform network by exploiting any of the vulnerabilities identified in the reconnaissance stage.
- Command and Control: once inside of the platform, the attacker typically would install any malicious software, such as remote access tools, in order to quickly access again to the system with very few resources.
- Escalate privileges: attackers typically try to escalate their privileges once inside the system, for example, by obtaining PKI certificates or with the installation of key loggers to obtain passwords.
- Move Laterally: attackers scan the network internally in order to find additional targets, for example, to access to other devices and performing internal vulnerability scans.
- Target Attainment: attackers finally gets access to the pursued resources, either retrieval or deletion of files or info from databases, or simply resetting configurations or shutting down devices.

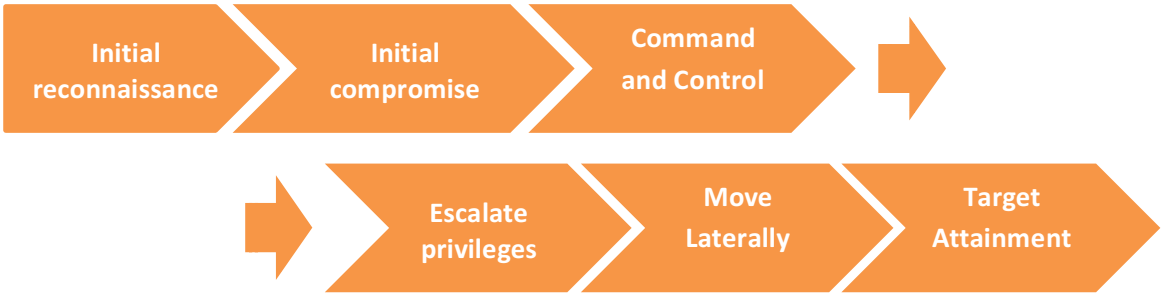

Figure 13: Cyber Attack lifecycle

5.4.3 Security objectives for IoT/CPS

The third pillar to analyse is related to the security objective that has to be reached for the protection of an IoT/CPS against threats and attacks. According to [Wang10], four objectives typically targeted:

- Confidentiality, in order to prevent the disclosure of sensible information (including the maintenance of user's privacy) to unauthorized individuals or systems.
- Integrity, in order to ensure that the data managed in the system have not been altered by unauthorized parties.
- Availability, in order to ensure that the services provided in IoT/CPS platforms or the resources offered by devices are working properly without interruptions.
- Authenticity, in order to ensure that all the processes (data management, transactions, and communications) are genuine and produced/consumed by trusted parties.

5.4.4 Main threats in IoT/CPS

A myriad of cyberattacks are threatening IoT/CPS infrastructures. Almost every week some relevant new incident involving cyber-attacks and IoT appears in the mass media. One of the first proven massive cyberattacks in IoT happened in 2014, when 750.000 malicious emails were sent from 100.000 from devices such as TVs or refrigerators. In October 2015 a massive DDoS attack, triggered from smart light bulbs, webcams or smart thermostats, affected important DNS servers in the USA. Many cyberattacks have also targeted IoT infrastructures built over critical infrastructures. The most salient one occurred already in 2010 when the so called Stuxnet ruined several nuclear centrifuges of nuclear power plants by exploiting several vulnerabilities present in access control devices. More recently, in the winter of 2015, a Ukrainian power grid suffered the so called Blacknet attack. The attack managed to install malware in many devices within the power grid premises. The result was the complete blackout of an entire city. Another massive DDoS attack triggered from many different devices took down for a week in November 2016 the central heating system of a Finnish city.

Typical approaches to analyse security threats and vulnerabilities in IoT/CPS divide these platforms into three conceptual layers: physical layer, network later and application layer [Gao13]. The following tables summarize the most important threats for IoT/CPS and group them according to the layer where they are applied:

Table 2: Security Threats of Physical Layer

Security threats	Description
Physical attack	Physical attack mainly refers to the physical damage for the nodes.
Equipment failure	Equipments reduce or lose performance due to external forces, environment or aging.

Line fault	Line failure is the failure of power lines on the nodes.
Electromagnetic leakage	By processing electromagnetic signal equipments at work radiated out, attackers can restore the original data.
Electromagnetic interference	Unwanted electromagnetic signals or commotions make negative impacts on useful signals, resulting in system performance degradation.
Denial of Service (DoS)	Attacker makes the target system stop providing services through network bandwidth consumption.
Channel blocking	Data cannot be transmitted for communication channel has been occupied for a long time.
Sybil attack	Single malicious node has multiple identities, to attack the system by controlling most of the nodes.
Replay attack	Attacker resends the legitimate data obtained before, to get the trust of the system.
Perception data destruction	The unauthorized addition, deletion, modification and destruction of perception data.
Data intercept	Illegal access to the data resources through intercepting the communication channel.
Data tampering	Attacker intercepts and modifies the data, then sends modified data to the recipient.
Unauthorized access	Resources are accessed by unauthorized users.
Passive attack	Attacker passively collects data by sniffing and information collection.
Node capture	Gateway node or ordinary node is controlled by attackers.

The following table lists the typical security threats that are focused on the network layer.

Table 3: Security Threats of Network Layer

Security threats	Description
DDoS	Plenty of malicious nodes attack target server as the sources of DoS at the same time.
Routing attack	Attacker interferes with the normal routing process by sending forged routing information.
Sink node attack	Interrupting data transmission between physical layer and network layer by attacking the sink node.
Direction misleading attack	Malicious node modifies the source and destination addresses of data packets then sends it to a wrong path, resulting in network routing confusion.

Black hole attack	Malicious node cheats other nodes to establish routing connections with it, and then discard the packet should be forwarded, causing packet loss.
Flooding attack	Exhausting the resources of the network servers on network layer by Smurf and DDoS.
Trapdoor	Allow the exception of security policy when specific data transporting.
Sybil attack	Malicious node illegally has multiple identities, to obstruct data transmission by controlling most of the nodes.
Sinkhole attack	Malicious node attracts normal nodes around as a point in the routing path, so that all data will flow through it.
Wormhole attack	Malicious nodes attack together to get the routing right by the less routing hops between the malicious nodes.
Routing loop attack	Malicious node modifies the data path to cause an infinite routing loop.
HELLO flooding attack	Malicious node makes nodes in the network aware that it is their direct neighbour by using strong signal to broadcast routing information.
Spoofing attack	Malicious node spoofs normal nodes to send data through an inefficient path or to a failure node.
Selective forwarding	Malicious node deliberately loses some or all of the key information in the forwarding.
Tunnel attack	Malicious nodes hide the real link distance between them to lure the other nodes to establish routing path through them.
False routing information	Malicious node attacks network layer network by tampering with the routing information.

Finally, the following table lists the typical security threats that are focused on the application layer.

Table 4: Security Threats of Application Layer

Security threats	Description
Privacy data leaking	Leaking of privacy data of users due to the insecurity of data transmission, storage and presentation.
Unauthorized access	Illegal access to the network and system data.
Malicious code	Code in the system with no effect but may have security risks.
Forged control commands	Attackers maliciously use the system or damage the system by forging control commands
Loophole	Attacking the system by using the loopholes in the applications on application layer.

Viruses, Trojan horses	Viruses and Trojan horses are the generally security threats of applications on application layer.
SQL injection attack	SQL injection is a common mean of attack on database of the system.

5.4.5 Common countermeasures to mitigate threats in IoT/CPS

A countermeasure is defined as an action taken to weaken the effect of another action or a situation, or to make it harmless. In general, threats are unavoidable and every system has to be designed with the assumption that it will often suffer from many different types of attacks. According to [Cardenas09], the growing concern for protection IoT/CPS against malicious cyberattacks is based upon the premises of prevention, detection, recovery, resilience and deterrence.

Prevention is the first defence against cyberattacks, and becomes a challenge mostly targeted by the standardization community from many different domains. Some examples are the cybersecurity standard for controls systems in the Electric sector created by the North American Electric Reliability Corporation (NERC). NIST has also published a set of best practices in the NIST SP 800-53, with a set of recommendations that can provide guidance for analysing the security of most companies. The ISA (International Society of Automation) is developing the ISA99, which includes a set of s standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance, with the objectives of improving confidentiality, integrity and availability of control systems.

The detection and recovery against attacks is the main reaction countermeasure to address when an attack has succeeded. The usage of monitoring tools becomes the first mechanism to detect attacks. To this end, a key aspect for detecting attacks is the deep knowledge of the system. Very often this is done through human intervention, although the need of automatic recovery becomes one of the paramount challenges being currently targeted by industry.

System resilience, together with security by design principles, becomes another important aspect used to react or prevent attacks. Some specific actions related to this aspect are the redundancy (to prevent singles point of failure), diversity (having the same service running on different SOs), or the limitation of privileges (separating privileges among different users to limit the access that a corrupted entity can have to the system and its resources).

Not being the most successful measure to prevent or react to attacks, deterrence becomes the basic aspect that any domain should have. However, very often this aspect depends on successful legislation, law enforcement and international collaboration, which have been proved not to be effective enough to prevent cyber-attacks.

The specific case for IoT is very challenging given the diversity of operative systems, interfaces, and capabilities for the devices operating in an IoT platform. A common strategy to react to threats is only possible through the unification of all the access modes available at every device. To this end, the usage of SDN and NFV technologies becomes essential for the definition and invocation of countermeasures that allows to react to ongoing attacks or potential threats. Actions such as the isolation of compromised devices (in order to avoid a potential extension of the attack to critical parts of the platform), the reconfiguration of certain parts of the IoT platform (for example, assigning different IPs to comprised devices), the restart of some devices or the change of access policies at runtime are some of the possible actions to be carried out when reacting to attacks such as DoS, malware, etc.

6 LEGISLATIVE AND SOCIOLOGICAL PERSPECTIVE ANALYSIS

Digital interactions are fundamentally linked to trust and security. The widespread adoption and evolution of ICT has led to both an increase in innovative activities across all sectors; and the continuously expansive reach of security vulnerabilities and risks. As recent events and security breaches[26] have caught the media's attention; discussions on the (in)security of network and information systems, have become commonplace. This in turn has stirred increasing levels of concern among the public, who more now than ever claim for viable solutions capable of restoring their trust and protecting their security.

Despite this situation, there is no simple answer capable of ensuring total ICT security, "Security is not achieved by a single technical fix, nor can it come about because one company or sector of the economy decides security is important. Creating security and trust in the Internet requires different players (within their different responsibilities and roles) to take action closest to where the issues are occurring"[27].

As traditional approaches based only on technical solutions give way to holistic approaches, a trend towards the involvement of end-users into the creation of secure ICT environments is now focused on fostering a security mindset that embeds security considerations into the everyday choices of users[28].

In this context, informing and conveying trust to security-aware users has become more relevant than ever. In the words of Robert Hayes, "Trust is at the heat of a successful security strategy, yet knowing who and what can be trusted, and whether that trust should be absolute or conditional, is extremely difficult"[29]. A holistic approach to security, aimed at empowering and educating end users will require the creation of tools designed to facilitate end-user trust.

A leap forward towards this direction can be achieved through the introduction of end-user iterative security validation tools. Through the integration of technical, educational and methodological solutions, end-users are not only given the opportunity to monitor the status of the ICT systems that are most relevant to them; but also, to take preventative and curative steps towards securing their information from cyberattacks.

Network and information systems and services are increasingly at risk, the more they play a vital role in our society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the market as well to the protection of rights and liberties of individuals whose information circulate in those networks.

In the light of this, the European Union is in the process of reviewing the regulatory framework governing the cybersecurity and the protection of personal data.

In 2016, the European Union legislator adopted Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (hereinafter "NIS Directive"). The Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;

[26] See https://dig.watch/issues/cybersecurity
[27] Internet Society (2015), Internet Society approach to cyber security policy, https://www.internetsociety.org/news/internet-society-approach-cyber-security-policy
[28] Dutton, William (2017), Fostering a Ccyber security mindset. https://policyreview.info/articles/analysis/fostering-cyber-security-mindset
[29] Hayes, Robert (2016), Cybersecurity: a question of trust. https://blogs.microsoft.com/microsoftsecure/2016/10/20/cybersecurity-a-question-of-trust/

- cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
- a culture of security across sectors which are vital for the economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. **Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority**. **Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive**. This should include also providers of IoT services and products.

Further to the NIS Directive, the relevant European legal framework also protects personal data against data breaches, by means of security obligations imposed on undertakings by Regulation 679/2016 (hereinafter "GDPR"). More specifically, and regardless of the role they bear within the personal data processing, organizations in Europe must implement **appropriate technical and organizational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

A strategy which embeds the protection of personal data – also in terms of security – into the design and functioning of the systems, needs therefore to be devised and followed.

The strategy should incorporate the following elements:

a) **clear allocation of roles** within the personal data processing, in order to:
   a. identify the data controller, the data processor(s) and the persons processing personal data under the authority of the controller or processor;
   b. formally bind the data processor(s) to guarantee a certain level of safeguards for personal data;
   c. map any potential stakeholder that may process personal data outside the European Union and formally bind it to guarantee a certain level of safeguards for personal data;
   d. assign the relevant authorization and authentication profiles to the persons processing personal data under the authority of the controller or processor.

b) appointment of a **Data Protection Officer**, where necessary, in the light of the business and related data processing activities carried out by the data controller and/or processor;

c) a **Data Protection Impact Assessment** (DPIA), where necessary; this process is anyway recommended for services, applications, systems that process personal data, even though they do not seem risky at the outset. The DPIA is a crucial step to ascertain whether personal data run risks in terms of security, and what the remedies are to those risks;

d) implementation of the principles of **data protection by design and by default** throughout the whole data lifecycle;

e) **policies and procedures to periodically test the security** resilience of a system (e.g., penetration tests, vulnerability assessments, etc.) and carry out the relevant remediation activities;
f) adherence to codes of conduct and /or certification mechanisms for security of personal data
g) a well defined internal procedure to cope with any **data breaches and notification thereof**:
    a. to the competent Data Protection Authority, within 72 hours after having become aware of it;
    b. to the data subjects involved, without undue delay, unless any of the following conditions are met:
        i. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
        ii. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
        iii. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

On top of this, the revision of rules for privacy in the electronic communications sector shall be followed, as the European Union is planning to replace the currently in force Directive 2002/58/EC with a Regulation that should extend privacy and security obligations to the so called "over-the -top" providers too.

This regulatory approach is framed within the Digital Single Market Strategy pursued by the European Commission, which encompasses **Internet of Things** developments too. According to the recent Commission's Communication on this subject: [30]

"The Commission will consider the possible need to adapt the current legal framework to take account of new technological developments (including robotics, Artificial Intelligence and 3D printing), especially from the angle of civil law liability and taking into account the results of the ongoing evaluation of the Directive on liability for defective products and the Machinery Directive. Predictability on the access to patent protected technology endorsed in standards (standard essential patents) is key for the rollout of Internet of Things where a broad range of sectors will implement standards on mobile connectivity. The Commission is assessing effective means to ensure a balanced framework for the licensing of this intellectual property respecting the interests of both developers and users of technology.

The Commission will:

- *by autumn 2017, subject to Impact Assessment, prepare a legislative proposal on the EU free flow of data cooperation framework which takes into account the principle of free flow of data within the EU, the principle of porting non-personal data, including when switching business services like cloud services as well as the principle of availability of certain data for regulatory control purposes also when that data is stored in another Member State;*

[30] COM (2017) 228 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy.

- *in spring 2018, based on an evaluation of existing legislation and subject to an Impact Assessment, prepare an initiative on accessibility and re-use of public and publicly funded data and further explore the issue of privately held data which are of public interest.*
- *also further analyse whether to define principles to determine who is liable in cases of damage caused by data-intensive products.*
- *continue to assess the need for action concerning the emerging data issues as identified in the data Communication from January 2017, such as data access rights".*

The regulatory framework described above is evidently in a transitional phase and requires to be closely followed by any interested party and proactively implemented in the daily business activities, in order to ensure not only formal compliance with the rules yet substantial protection to the systems and the personal data they carry.

7 SECURITY IN ANASTACIA

In this section of the document we will try to contextualize security aspects previously considered, by mapping them on the expected implementation of the ANASTACIA platform.

7.1 ANASTACIA PROTECTION LAYERS

Concerning the development of the ANASTACIA platform, the deploy of efficient protection systems is crucial in order to effectively identify and mitigate threats targeting the system. In this context, it is important to exploit already available consolidated solutions, with the aim of avoid repeated design, engineering and implementation of already available components. Such approach leads to focus on the development of innovative components of the system. In this context, three different kinds of protection components can be considered, in order to implement security on top of three different layers:

- Consolidated components off the shelf (COTS)
  The first protection layer focuses on the adoption of consolidated solutions provided by network and security vendors. Although such exploitation does not represent an innovative characteristic for the ANASTACIA platform, it provides efficient security solutions against well known threats, today mitigated by different vendors. For instance, it is worth to mention that during the development of this document, an important cyber-security event occurred. Indeed, in May 2017, the WannaCry ransomware was discovered, targeting several companies around the world and encrypting data on the targeted devices and replicating itself through vulnerable systems sharing data on the network. The attack, exploiting a recent but known vulnerability, caused serious damages to a wide range of companies around the globe. Nevertheless, at time of first target, the attack was already mitigated by some vendors of network appliances (e.g., Sonicwall). By considering this sample, it is important to avoid to “reinvent the wheel”, by exploiting already available COTS components (to be kept continuously updated) that are able to provide protection to a wide range of well known threats.
- Already available partners’ products and systems
  The second protection layer is focused on the adoption of products and services already implemented by the partners of the project. Unlike the previous case, the adoption and execution of such tools is not available to the mass. In this context, the Montimage Monitoring Tool (MMT) implemented by Montimage, represents a software able to analyse network traffic and extract protocols metadata. By using Deep Packet and Flow Inspection techniques (DPI/DFI), it’s possible to extrapolate metadata given in input to other modules of the tool. Such tools, not necessarily available publicly, provide an important contribution during the security implementation activities, due to the innovative characteristics of the tool themselves.
- Innovative protection solutions
  The last protection layer to be considered during the development of ANASTACIA security aspects is related to the design and development of innovative protection systems. The ANASTACIA platform will benefit from research activities executed in order to implement novel algorithms and systems able to counter cyber-attacks. In this context, the work will be focused on studying two categories of attacks in particular: from one side, Denial of Service (DoS) attacks, executed in order to make a network service not available to legitimate users; the focus is here on recent categories of attacks known as low-rate DoS, or Slow DoS Attacks. On the other side, covert channels will be investigated; such attacks are executed in order to bypass network restrictions or to exfiltrate sensitive information outside of the organization network. Both these kinds of threats represent a serious danger for the entire ANASTACIA platform. The focus will concern the study of the threats and the identification of running attacks, by analysing the network live traffic.

7.2 CURRENT ANASTACIA PROGRESS

In this section of the document we focus on the technical aspects of the ANASTACIA framework with the aim of analyse the current state of the ANASTACIA framework development, accordingly to the results achieved in the other running WPs.

Accordingly to the following figure, we focus on the technical WPs, hence, on WP2 "Security and Trust by Design Enablers", WP3 "Policy Enforcement and Run Time Enablers", WP4 "Monitoring and Alert/Reacting Enablers", and WP5 "Dynamic Security and Privacy Seal".

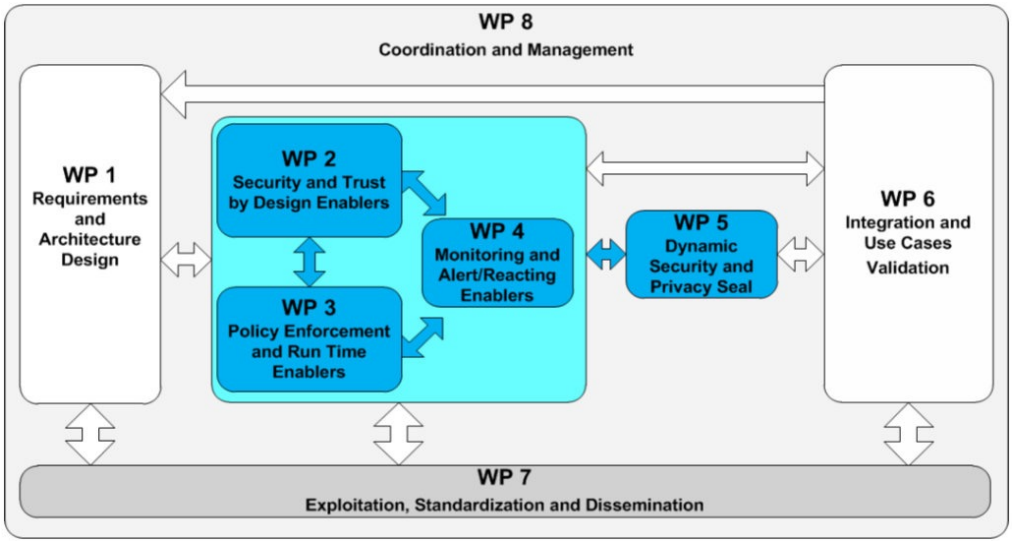

Figure 14 - Focus on current ANASTACIA development analysis

We will now briefly describe the progress status of the mentioned WPs.

7.2.1 WP2 "Security and Trust by Design Enablers"

The aim of the WP2 is to define the orchestration policies for SDN and IoT contexts, to analyze and focus on specific attack threats and mitigation measures, to investigate privacy risk models and associated contingency plans, and to provide a set of secure software development guidelines and procedures. Following considerations have been made so far.

- Policy definition and policy for orchestration
  Two policy languages, previously described, have been considered: X-CIM (Common Information Model), the main DMTF standard that provides a common definition of management-related information independent of any specification, and HSPL/MSPL (High-level Security Policy Language and the Medium-level Security Policy Language), language policies defined within the European SECURED project. Moreover, a comparison between the most adopted SDN controllers and the most relevant open-source NFV-MANO has been accomplished. Finally, a prototype focused on isolating devices from SDN networks has been implemented. Such prototype has been developed by adopting HSPL/MSPL policies and specific OpenDayLight SDN plugins.
- Attack threat selection
  The focus is on last generation threats and in particular on low-rate denial of service (DoS) attacks and cover channels technologies. As previously mentioned, low-rate DoS threats are emerging attacks targeting network server systems with the aim of making them unreachable. The novelty of the attacks and their behaviour, similar to the behaviour of a legitimate client communicating on the network, makes them extremely difficult to counter. On the other side, covert channels, executed in order to break the network in order to access filtered services, or by insider threats to

export sensitive data outside of the organization network, are also particularly difficult to identify, since the malicious payload is encapsulated on unfiltered protocols packets.

- Attacks mitigation
  By considering in particular intrusion detection systems (IDS), two different approaches are considered: signature based detection, generating signatures of well known threats in order to identify them, and anomaly based detection, distinguishing between legitimate and anomalous scenarios by comparing specific metrics computed from live traffic with the computation of a legitimate traffic.

7.2.2 WP3 "Policy Enforcement and Run Time Enablers"

The aim of the WP3 is to design and develop algorithms, protocols and mechanisms to orchestrate the required security functions, according to the desired policies. The security orchestrator implemented in WP3 is a crucial element of the ANASTACIA platform, to efficiently manage the deployment and configuration of security mechanisms in complex scenarios like SDN, NFV, and IoT. In this vein, the following considerations have been made.

Policy Refinement Procedures for Security Enablers Orchestration Security capabilities define the set of network security functions NSF (VNF if they are virtual) that will enable the selected policies requirements. These security capabilities allow to describe the security features of the system in a technology-agnostic way, without the need to designate specific implementations. A NSF/VNF, also called security enabler, implements security controls. High-level Security Language (HSPL) is translated into security controls through a two steps process using a Medium-level security Policy Language (MSPL) first, hence applying a conversion from MSPL to certain enabler security controls. The low-level configuration can be then used to effectively orchestrate the required security enablers.

- Orchestration of Security Functions
  Accounting for the heterogeneity of available security enablers, the ANASTACIA orchestration is in charge of efficiently managing the enforcement over different environments, such as NFV, SDN, IoT. To this aim, specific efforts have been addressed to investigate the interactions with relevant control and management modules. In case of SDN, the Northbound APIs of SDN controller can be exploited to enforce relevant SDN flow rules, as well as to receive statistic information from the underlying SDN switches. To deploy and configure security VNFs, the ANASTACIA orchestration can refer to the Management and Orchestration (MANO) block of the ETSI ISG NFV architecture, whose features have been detailed in Section **Errore. L'origine riferimento non è stata trovata.**. To manage security controls in the IoT domain, the ANASTACIA orchestration will rely on specific IoT controllers, which can communicate with the IoT devices via different IoT management protocols, such as Constrained Application Protocol (COAP), Lightweight Machine to machine (LWM2M), RESTCONF.

7.2.3 WP4 "Monitoring and Alert/Reacting Enablers"

The aim of WP4 is to implement monitoring, alert and reaction components/enablers of the ANASTACIA platform. Following activities characterize the work behind WP4 development.

- Monitoring module design
  The architecture of the module has been defined. The module will be implemented to detect security issues by adopting a signature-based strategy, analysing the network traffic and looking for abnormalities by using the signatures database. A data analysis module belonging to the monitoring module component makes use of DPI/DFI technologies to test the rules defined in the signatures database. The output of the module includes the list of verdicts of the tested properties.
- Alert, reaction and detection module design

The architecture of the module has been defined. Such module is a core element of the ANASTACIA platform, as it analyses the verdicts received by the monitoring module, hence proposing countermeasures and raising alerts, where needed.

7.2.4 WP5 "Dynamic Security and Privacy Seal"

The aim of the WP5 is to research, analyse, design, develop and implement an innovative model of Dynamic Security and Privacy Seal that combines the obligations from the new European General Data Protection Regulation (GDPR) and other relevant normative dispositions, ISO norms and ITU recommendations; together with real time monitoring of deployed systems, including a quantitative and qualitative run-time evaluation of the quality of security and privacy risks, which can be easily understood and controlled by the final users.

The Dynamic Security and Privacy Seal will be closely integrated with the rest of the ANASTACIA architecture. Several considerations have been made so far.

- Legal Obligations and Norms

  Relevant normative dispositions on privacy and cybersecurity have been identified in the international, regional and national level, particularly through the GDPR, e-Privacy Directive, NIS Directive and Swiss Law. Research will focus on the specific interplay between these normative bodies and the standards/models considered below.

- Standards and Models to be Considered

  Various ISO Standards and ITU-T recommendations have been identified and noted as potentially relevant, these will be analysed in parallel to a number of Privacy Impact Assessment Methodologies, Threat Analysis Models and the principles and recommendations generated by relevant stakeholders on IoT security and privacy. Once clarity has been achieved on the contextual framework, research will focus on synthetizing the Privacy and Security requirements that must be addressed by the Seal, will along with the listing of the risks and threats to be monitored.

- Dynamic Security and Privacy Seal (DSPS) Model

  WP5 will then explore the possibility to combine ISO and regulatory requirements with real time monitoring. A specific model will be designed and specified. Several options may be considered, including completely ICT-based models and hybrid models where on-site human inspection can complement ICR tools. Once a solution that meets these requirements is found, identification of relevant Anastasia enablers capable of addressing the list of risks and threats to be monitored will take place. Finally, a set of specifications to further define the process and user interface will be generated along with the technical requirements for the DSPS implementation.

- Dynamic Security and Privacy Seal (DSPS) Implementation

  Once the model will have been clearly specified, WP5 will start implementing the seal as a highly trustable and authenticated dynamic seal. WP5 will most likely adopt the perspective of an external service located in a secured server and connected to the distributed ANASTACIA platforms with highly secured and authenticated access. Later on, WP5 will focus on the user interface and experience by leveraging real use cases.

8 CONCLUSIONS

In this document, we have analysed ANASTACIA security framework structure, by considering a holistic view, through the adoption of a holistic cyber-security approach. We have first introduced ANASTACIA technical details, hence formalizing and describing HCS-IF, the Holistic Cyber-Security Implementation Framework adopted.

We have then discussed the Building Energy Management System (BEMS), Multi-access Edge Computing (MEC), and Internet of Things (IoT) scenarios considered in ANASTACIA, by evaluating, from users' perspective, their characteristics and analysing how the ANASTACIA platform can provide added value, in terms of security provided to the system. Then, we have considered business aspects related to the ANASTACIA platform, by analysing the profit and advantages the system can provide to the stakeholders, from the business point of view. We have also analysed technical aspects of ANASTACIA, with particular focus on security and data privacy and management, discussing network security enablers security aspects and threats to be considered, with special focus on IoT environments. Also, we have studied legislative and sociological aspects of ANASTACIA, by analysing security related regulations and considering the importance of providing trust to security aware users.

The detailed analysis accomplished during the development of ANASTACIA Task 1.1 and described in this document will result a crucial element for the development of the entire platform, due to the multi-aspect point of view.

9 APPENDIX I: SECURITY RELATED TERMINOLOGY

In the following, accordingly to the NIST glossary of key information security terms [Nist, 2013], we report a selected subset of terms related to the cyber-security context.

Term	Definition
Access Authority	An entity responsible for monitoring and granting access privileges for other authorized entities.
Access Control List (ACL)	1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. 2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.
Access Point	A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.
Account Management, User	Involves: the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; managing these functions.
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non- repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Ad Hoc Network	A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station.
Add-on Security	Incorporation of new hardware, software, or firmware safeguards in an operational information system.
Advanced Encryption Standard (AES)	The Advanced Encryption Standard specifies a U.S. government- approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits.
Anomaly-Based Detection	The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
Attack Sensing and Warning (AS&W)	Detection, correlation, identification, and characterization of intentional

	unauthorized activity with notification to decision makers so that an appropriate response can be developed.
Attack Signature	A specific sequence of events indicative of an unauthorized access attempt.
Attribute-Based Access Control	Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.
Authentication Protocol	A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier
Automated Security Monitoring	Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.
Backdoor	Typically unauthorized hidden software or hardware mechanism used to circumvent security controls.
Baseline Security	The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.
Black Box Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.
Black Core	A communication network architecture in which user data traversing a global Internet Protocol (IP) network is end-to-end encrypted at the IP layer.
Blended Attack	A hostile action to spread malicious code via multiple methods.
Blinding	Generating network traffic that is likely to trigger many alerts in a short period of time, to conceal alerts triggered by a "real" attack performed simultaneously.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Brute Force Password Attack	A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords
Buffer Overflow Attack	A method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt data in memory.
Bulk Encryption	Simultaneous encryption of all channels of a multichannel telecommunications link.

Callback	Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and re-establishes contact.
Central Services Node (CSN)	The Key Management Infrastructure core node that provides central security management and data management services.
Certificate	A digital representation of information which at least 1)identifies the certification authority issuing it, 2) names or identifies its subscriber, 3) contains the subscriber's public key, 4) identifies its operational period, and 5) is digitally signed by the certification authority issuing it.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates
Cipher Block Chaining-Message Authentication Code (CBC-MAC)	A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic.
Claimant	A party whose identity is to be verified using an authentication protocol.
Closed Security Environment	Environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an information system life cycle. Closed security is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control.
Cloud Computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self- service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).
Common Misuse Scoring System (CMSS)	A set of measures of the severity of software feature misuse vulnerabilities. A software feature is a functional capability provided by software. A software feature misuse vulnerability is a vulnerability in which the feature also provides an avenue to compromise the security of a system.

Common Vulnerabilities and Exposures (CVE)	A dictionary of common names for publicly known information system vulnerabilities.
Communications Cover	Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.
Communications Profile	Analytic model of communications associated with an organization or activity. The model is prepared from a systematic examination of communications content and patterns, the functions they reflect, and the communications security measures applied.
Communications Security (COMSEC)	A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.
Community Risk	Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as **white box testing**.
Computer Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
Computer Network Attack (CNA)	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Computer Network Defense(CND)	Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control	Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
Content Filtering	The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.
Continuous Monitoring	The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording

	changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information-sharing decisions involving the enterprise.
Counter with Cipher Block Chaining-Message Authentication Code (CCM)	A mode of operation for a symmetric key block cipher algorithm. It combines the techniques of the Counter (CTR) mode and the Cipher Block Chaining-Message Authentication Code (CBC-MAC) algorithm to provide assurance of the confidentiality and the authenticity of computer data
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cover-Coding	A technique to reduce the risks of eavesdropping by obscuring the information that is transmitted.
Covert Channel	An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel.
Critical Infrastructure	System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Cross Site Scripting (XSS)	A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptanalysis	1) Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. 2) The study of mathematical techniques for attempting to defeat cryptographic techniques and information system security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.
Cryptographic Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and 2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the

	purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks.
Cyclical Redundancy Check (CRC)	A method to ensure data has not been altered after being sent through a communication channel.
Data Encryption Standard (DES)	Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. (FIPS 46-3 withdrawn 19 May 2005) See Triple DES.
Data Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
Data Security	Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.
Defense-in-Breadth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)
Digital Forensics	The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.
Distributed Denial of Service (DDoS)	A Denial of Service technique that uses numerous hosts to perform the attack.
Eavesdropping Attack	An attack in which an Attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the Claimant.
Embedded Cryptographic System	Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem.

Encrypted Network	A network on which messages are encrypted (e.g., using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties.
Encrypted Key	A cryptographic key that has been encrypted using an Approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.
End-to-End Encryption	Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible.
Exploit Code	A program that allows attackers to automatically break into a system.
Exploitable Channel	Channel that allows the violation of the security policy governing an information system and is usable or detectable by subjects external to the trusted computing base.
Firewall	A gateway that limits access between networks in accordance with local security policy
Firewall Control Proxy	The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call, and direct the firewall to close these ports at call termination.
Firmware	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
Flooding	An attack that attempts to cause a failure in a system by providing more input than the system can process properly.
Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
Formal Method	Mathematical argument which verifies that the system satisfies a mathematically-described security policy.
Gateway	Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.
Hacker	Unauthorized user who attempts to or gains access to an information system.
Handshaking Procedures	Dialogue between two information systems for synchronizing, identifying, and authenticating themselves to one another.
Hash Function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1) One-Way. It is computationally infeasible to find any input that maps to any prespecified output. 2) Collision Resistant. It is computationally infeasible to find any two distinct

	inputs that map to the same output.
Hash-based Message Authentication Code (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function.
Identity-Based Access Control	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Systems Security Engineering (ISSE)	Process of capturing and refining information protection requirements to ensure their integration into information systems acquisition and information systems development through purposeful security design or configuration.
Intrusion Detection Systems (IDS)	Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
IP Security (IPsec)	Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.
Jamming	An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable.
Kerberos	A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.
Key Distribution Center (KDC)	Communication security facility generating and distributing key in electronic form
Key Establishment	The process by which cryptographic keys are securely established among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).

Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.
Key Transport	The secure transport of cryptographic keys from one cryptographic module to another module.
Keyed-hash based message authentication code (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function.
Labeled Security Protections	Access control protection features of a system that use security labels to make access control decisions.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Man-in-the-middle Attack (MitM)	An attack on the authentication protocol run in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them.
Mandatory Access Control (MAC)	A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity.
Message Authentication Code (MAC)	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non- repudiation protection.
Multi-Hop Problem	The security risks resulting from a mobile software agent visiting several platforms.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other.
Network Sniffing	A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
Off-line Attack	An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.

Off-line Cryptosystem	Cryptographic system in which encryption and decryption are performed independently of the transmission and reception functions.
Online Attack	An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.
Online Cryptosystem	Cryptographic system in which encryption and decryption are performed in association with the transmitting and receiving functions.
Organizational Information Security Continuous Monitoring	Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real-time, data-driven risk management decisions.
Over-The-Air Key Distribution	Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation.
Packet Sniffer	Software that observes and records network traffic.
Passive Attack	An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping).
Password Cracking	The process of recovering secret passwords stored in a computer system or transmitted over a network.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
Policy-Based Access Control (PBAC)	A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, and heuristics).
Policy Certification Authority (PCA)	Second level of the PKI Certification Management Authority that formulates the security policy under which it and its subordinate CAs will issue public key certificates.
Quality of Service (QoS)	The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service-Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements. Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.
Radio Frequency	A form of automatic identification and data capture (AIDC) that uses electric or

Identification (RFID)	magnetic fields at radio frequencies to transmit information.
Replay Attacks	An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.
Risk Analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Role-Based Access Control (RBAC)	A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.
Root Certification Authority	In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Rootkit	A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.
Sandboxing	A method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain
Secure Hash Algorithm (SHA)	A hash algorithm with the property that is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.
Secure Socket Layer (SSL)	A protocol used for protecting private information during transmission via the Internet. Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:."

Spoofing	"IP spoofing" refers to sending a network packet that appears to come from a source other than its actual source.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Steganography	The art and science of communicating in a way that hides the existence of the communication. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
Tunneling	Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and Web servers.
Trusted Agent	Entity authorized to act as a representative of an agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome).
Virtual Private Network (VPN)	A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Wi-Fi Protected Access-2 (WPA2)	The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For federal government use, the implementation must use FIPS-approved encryption, such as AES.

10 REFERENCES

[Ali, 2015] Ali, Syed Taha, et al. "A survey of securing networks using software defined networking." IEEE transactions on reliability 64.3 (2015): 1086-1097.

[Atoum, 2014] Atoum I., et al. "A holistic cyber security implementation framework", *Information Management & Computer Security,* 2014

[Bernal] Bernal J., et al. "Networking and Traffic Engineering in Emerging Distributed Computing Applications", Chapter 4 Security Policy Specification]

[Cardenas09] Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. In Workshop on future directions in cyber-physical systems security (p. 5).

[ETSI, 2015] ETSI. Mobile-edge computing (mec); proof of concept framework.2015.

[ETSI-NFV, 2014] ETSI GS NFV 002, Network Functions Virtualisation (NFV) - Architectural Framework, v. 1.2.1, 2014.

[ETSI-NFV-MANO, 2014] ETSI GS NFV-MAN 001, Network Functions Virtualisation (NFV) – Management and Orchestration, v. 1.1.1, 2014.

[Gao13] Gao, Y., Peng, Y., Xie, F., Zhao, W., Wang, D., Han, X., ... & Li, Z. (2013, October). Analysis of security threats and vulnerability for cyber-physical systems. In Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on (pp. 50-55). IEEE.

[Gold, 2009] Gold S., "The scada challenge: securing critical infrastructure", Network Security, 2009(8):18–20, 2009

[Kost14] Dimitar Kostadinov. Cyber Threat Analysis. Infosec Institute. July 2014. Online: http://resources.infosecinstitute.com/cyber-threat-analysis/. Last access: May 2017.

[LECC] Cyber Attack Lifecycle. Law Enforcement Cyber Center. Online: http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/. Last access: May 2017.

[Nist, 2013] NIST, Glossary of Key Information Security Terms (revision 2). DOI 10.6028/NIST.IR.7298r2, 2013. Online: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[Paridari, 2016] Paridari K., et al. "Cyber-Physical-Security Framework for Building Energy Management System", ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), 2016

[Sage17] Threat Lifecycle Management: Overview and Solutions. The Sage Group. 2017. Available online: http://thesagegrpmentoring.com/wp-content/uploads/sites/524/2017/03/Sage-Group-LE-Solutions-Threat-Lifecycle-Management.pdf. Last access: May 2017.

[Sherwood, 2009] Sherwood, R., Gibb, G., Yap, K. K., Appenzeller, G., Casado, M., McKeown, N., & Parulkar, G. (2009). Flowvisor: A network virtualization layer. OpenFlow Switch Consortium, Tech. Rep, 1-13.

[Taleb, 2014] Taleb, T. (2014). Toward carrier cloud: Potential, challenges, and solutions. IEEE Wireless Communications, 21(3), 80-91.

[Thales, 2017] Thales Data Threat Report, https://dtr.thalesesecurity.com, 2017

[Trois, 2016] Trois, C., Del Fabro, M. D., de Bona, L. C., & Martinello, M. (2016). A Survey on SDN Programming Languages: Toward a Taxonomy. IEEE Communications Surveys & Tutorials, 18(4), 2687-2712.

[Vallini] Vallini M, "Policy Specification", SECURED-FP7 project, D4.1

[Wang10] Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010, December). Security issues and challenges for cyber physical system. In Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing (pp. 733-738). IEEE Computer Society.

[Xia, 2017] Xia L., et al. “Information Model of NSFs Capabilities”, draft-xibassnez-i2nsf-capability-01, March 12, 2017

[Soomro, 2016] Soomro et al. "Information security management needs more holistic approach: A literature review." International Journal of Information Management 36.2 (2016): 215-225

[James, 2016] James et al. "CYBERSECURITY EDUCATION: A HOLISTIC APPROACH TO TEACHING SECURITY." Issues in Information Systems 17.2 (2016)